Whitehouse-Kyl-Mikulski-Graham Cybersecurity Proposal —
***Hardening Critical Infrastructure Systems* (Short Summary/Analysis)**

Summary

- The Whitehouse-Kyl (et al.) cybersecurity proposal claims to establish a "voluntary" cybersecurity program to harden critical infrastructure, but it would require owners and operators to take certain actions involuntarily.

- The proposal does not recognize that businesses already comply with multiple information-security rules. It fails to answer a fundamental question: Which policies would genuinely help businesses protect their systems and networks and make them more resilient?

- Businesses repeatedly say that greater information sharing would help their cybersecurity, not greater regulation. The proposal would increase the size and scope of government and add more regulations on industry.

- If senators truly seek a compromise that would constitute sound policy and protect critical infrastructure, they should pass the SECURE IT bill (S. 2151) and blend it with CISPA (H.R. 3523), which passed the House in April. These bills would positively change the status quo.

The Whitehouse-Kyl (et al.) legislative proposal is intended to reach a "compromise" between the Lieberman-Collins (pro-regulation) and the McCain-Hutchison (anti-regulation) groupings on the role and scope of government in regulating critical infrastructure to harden cyber networks and systems. However, there appears to be nothing new in the proposal that would engender widespread industry support. The proposal seems like a patchwork of provisions taken from the Lieberman-Collins bill (S. 2105) and other measures.

The proposal is characterized as "voluntary," coupled with liability protections for covered critical infrastructure (CCI). Still, the text makes clear that this program would compel CCI owners to take certain actions involuntarily. Indeed, a subset of CCI would be required by DHS and DOD — due to a vague "national security need" — to provide these departments with a third-party assessment of the infrastructure's cybersecurity posture.

Whitehouse-Kyl Proposal Is a Step in the Wrong Direction, Away From Smart Security

The proposal contains provisions that (1) would increase the size and role of DHS, (2) would mandate cybersecurity standards promulgated by the federal government, and (3) wouldn't necessarily improve U.S. cybersecurity. Threats to collective security change too rapidly for any framework of mandatory standards to keep up. Here are some of the problems with the proposal:

- **Regulations** — The proposal would authorize DHS, DOD, the Commerce Department, and sector-specific agencies to require CCI to adopt certain standards and best practices (called Baseline Performance Goals or BPGs). In theory, each BPG would be outcome

driven, not prescriptive. But, in practice, each would likely become prescriptive, compulsory, and out of step with real-time threats. The proposal does not recognize that the businesses community already complies with multiple information-security rules — from CFATS (Chemical Facilities Anti-Terrorism Standards) to FERC-NERC CIP (Federal Energy Regulatory Commission-North American Reliability Corporation Critical Information Protection) standards to SOX (Sarbanes-Oxley Act), and more.

- **Security vs. compliance** — The proposal would shift business resources from actual cybersecurity (risk management) to compliance. It would establish a Cybersecurity Protection Program (CPP) requiring critical infrastructure to self-certify to DHS that it meets relevant BPGs. A CPP certificate would be valid for 3 years, which is an arbitrary time frame.

- **"Name and shame"** — CCI that is subject to the ambiguous "national security need" provision must provide DHS and DOD the report of a third-party assessor stating that the critical infrastructure operator is meeting required BPGs. On top of this, the proposal would authorize DHS and DOD to publish the assessment "in an appropriate form," which is incredibly problematic. Publicly disclosing CCI's sensitive security information should be considered bad policy; and seeking to "name and shame" companies should be seen as counterproductive to smart and effective security.

- **Liability protections** — Advocates of the proposal argue that CCI owners who hold a CPP certificate would be afforded liability protections arising from external cyberattacks. However, the limitations on liability are good but not bulletproof and, thus, would still leave owners open to punitive and noneconomic damages.

- **Government procurement** — The proposal would instruct the federal government to consider the holding of current CPP certificates in procurement decisions, which could have negative consequences (e.g., supply-chain related) for many companies.

- **DHS bureaucracy** — The proposal envisions an Office of Cybersecurity Protection within DHS, adding to the layers of bureaucracy already present at DHS.

- **Costs** — The proposal relies on federal agencies to determine whether the standards and best practices, or BPGs, would be technically feasible and would not create a financial burden on critical infrastructure operators. Appropriate input from the private sector on economic decision making is unclear in the proposal.

True Compromise Would Blend SECURE IT and CISPA to Improve U.S. Security

Despite being described as a voluntary program joined with incentives, the Whitehouse-Kyl (et al.) proposal is headed in the wrong direction. Businesses repeatedly say that greater information sharing would help their cybersecurity, not greater regulation. If senators truly seek a compromise that would constitute sound policy, they should pass the SECURE IT bill and combine it with CISPA, which passed the House in April by a vote of 248-168 (Rs 206-28; Ds 42-140). Congress is standing in the way of policies that would enhance America's collective security.

(June 8 summary of May 30 legislative proposal)