SUMMARY OF CYBERSECURITY LEGISLATIVE PROVISIONS TO PROTECT CRITICAL INFRASTRUCTURE

The approach outlined in these staff discussion draft provisions first and foremost recognizes that protecting our nation's critical infrastructure from cyber threats is a responsibility shared by the private sector and the government. It recognizes that policies should encourage innovation in cyberspace and should build upon longstanding public-private partnerships, rather than seeking to recreate them. The approach enhances cybersecurity while ensuring that personal privacy and civil liberties are protected at all times, including in the event of a national cyber emergency.

In short, this staff language would establish a flexible and dynamic approach to protecting our critical infrastructure that would clarify existing authorities and responsibilities. It outlines a framework for securing our nation's most critical infrastructure that draws on the expertise of all relevant Federal agencies, allows for private sector companies to develop tailored solutions to their own cyber vulnerabilities, and establishes accountability and incentives for cybersecurity. The language includes the following elements:

- Sector-by-sector cyber risk assessments to identify and evaluate cyber threats, vulnerabilities, and possible consequences, in order to identify and prioritize the critical infrastructure networks to be protected with these provisions.

- Designation of "covered critical infrastructure," defined narrowly as systems and assets whose disruption could result in the interruption of life-sustaining services, catastrophic economic damage, or severe degradation of national security capabilities.

- Promotion of advisory standards, guidelines, and best practices for cybersecurity.

- Development of sector-specific risk-based cybersecurity performance requirements for covered critical infrastructure that allow private sector companies to tailor their own solutions to meet these requirements.

- Establishment of evaluation and enforcement mechanisms to assure the public and the market.

- Development of response, resiliency, and preparedness for national cyber emergencies.

Sector-by-Sector Cyber Risk Assessments:

On a sector-by-sector basis, the Secretary of Homeland Security would work closely with the owners and operators of critical infrastructure and coordinate with the Intelligence Community and other key Departments, sector-specific agencies, and primary regulators to perform risk assessments of critical infrastructure systems and assets to identify and evaluate cyber threats, vulnerabilities, and consequences. These sector-by-sector risk assessments would

help inform the identification and prioritization of critical infrastructure systems and assets that, if disrupted or destroyed, could cause a major catastrophe.

Designating Covered Critical Infrastructure:

Drawing on these risk assessments, and continuing to work closely with the private sector and other key Federal agencies, the Secretary would designate the most critical infrastructure networks whose disruption would cause a major catastrophe. The definition focuses on specific critical infrastructure systems and assets, not entire organizations or companies. Only systems and assets whose disruption could result in one of the following severe consequences would be designated as "covered critical infrastructure":

- the interruption of life-sustaining services that would cause a mass casualty event or mass evacuations;
- catastrophic economic damage to the United States; or
- severe degradation of national security or national security capabilities.

The staff discussion draft provides for a robust administrative process for an owner or operator to challenge the designation of a system or asset as covered critical infrastructure and expressly permits challenges of a final agency determination in federal court.

Sector-Specific Risk-Based Cybersecurity Performance Requirements:

Rather than setting specific standards or a one-size-fits-all approach to cybersecurity, the discussion draft would require the Secretary to work with the private sector and other key Federal agencies to develop sector-by-sector, risk-based cybersecurity performance requirements to mitigate identified cyber risks. These requirements would be performance-based, not technology-based, to ensure that they are not out-paced by the advancement of technology. Owners and operators of covered critical infrastructure would develop and implement their own security measures to implement to meet applicable risk-based performance requirements, tailored to the specific cybersecurity needs of their company and networks. Owners and operators of covered critical infrastructure would be required to report cyber incidents that could pose a significant risk of disruption to the reliable operation of their covered networks. This information would be protected from unauthorized disclosure.

Evaluation and Enforcement:

An owner or operator of covered critical infrastructure would be required to certify annually to DHS and the company's primary regulator whether it has developed and implemented cybersecurity measures that satisfy the risk-based cybersecurity performance requirements. DHS would be authorized to perform spot assessments of covered critical infrastructure, or to delegate this authority to another relevant Federal agency. The staff discussion draft authorizes primary regulators, and DHS when the covered critical infrastructure does not have a primary regulator, to initiate enforcement actions against covered entities found to be in violation of applicable risk-based cybersecurity performance requirements. Such enforcement actions may include civil penalties.

Two possible provisions in the staff draft pertaining to evaluation and enforcement are subject to ongoing discussions:

1. Third-party private sector assessments of covered critical infrastructure companies' cybersecurity measures.
2. Liability protection for covered critical infrastructure companies that meet the requirements.

Advisory Standards, Guidelines, and Best Practices:

The staff discussion draft would bolster the development of standards, guidelines, and best practices for managing cyber risk. It reinforces the existing role of the National Institute of Standards and Technology to work with industry, sector-specific agencies, and primary regulators to review and assist in the development of, and recommend changes to information security standards, guidelines, and best practices developed by private sector organizations, international and domestic standards setting organizations, and Federal agencies. These advisory standards, guidelines, and best practices would be risk-based and flexible, and take into consideration economic impact, including on small businesses. These advisory standards, guidelines, and best practices would be taken into consideration in the development of risk-based cybersecurity performance requirements for covered critical infrastructure.

National Cyber Emergencies:

The staff discussion draft provides a responsible framework, developed in coordination with the private sector, for the President to authorize emergency measures, limited in both scope and duration, to protect the nation's most critical infrastructure if a cyber vulnerability is being exploited or about to be exploited. The President's ability to declare a national cyber emergency is limited to circumstances in which an actual or imminent cyber attack would disrupt covered critical infrastructure that would result in national or regional catastrophe. The President must notify Congress in advance about the threat and the emergency measures that will be taken to mitigate it. Any measures ordered must be the least disruptive means feasible. These emergency measures will expire after 30 days unless the President orders an extension, and they may not be extended for more than 90 days without a joint resolution of Congress. Owners and operators of covered critical infrastructure that are in compliance with the risk-based cybersecurity performance requirements would be protected from civil liability directly related to the implementation of emergency measures directed by the President. The bill does not authorize any new surveillance authorities, or permit the government to "take over" private networks. And, the bill states explicitly that the emergency authority shall not authorize the President, the Secretary, or any other Federal entity to "shut down" the Internet.