Administration Priorities for Cybersecurity Information Sharing Legislation

1) **Liability Protections**: The Administration supports providing narrowly targeted liability protections to incentivize broader cybersecurity threat information sharing. Appropriate liability protections should incentivize good cybersecurity practices and should not grant immunity to a private company for failing to act on information it receives about the security of its networks. Such a provision would remove incentives for companies to protect their customers' personal information and may weaken cybersecurity writ large. There is a danger that providing a good faith exception for a failure to act on information received could create a moral hazard and discourage companies from responding appropriately to cyber threat indicators they receive. Moreover, the standard of proof for liability in H.R. 1560 may be extraordinarily difficult to meet, thereby creating a disincentive for parties to exercise care in their use or dissemination of cyber threat information. **As such, the Administration strongly prefers the liability protections in S. 754.**

2) **DHS Portal**: The Administration supports authorizing new liability-protected sharing relationships only through the National Cybersecurity and Communication Integration Center (NCCIC), a civilian entity within the Department of Homeland Security. Additionally, the Administration supports real-time sharing between the NCCIC and relevant Federal agencies, with appropriate privacy protections, and has preliminarily deployed such a capability at DHS. Focusing real-time sharing through one center at DHS enhances situational awareness, facilitates robust privacy controls, and helps to ensure oversight of such sharing. In addition, centralizing this sharing mechanism through DHS will facilitate more effective real-time sharing with other agencies in the most efficient manner. Legislation that designates multiple points of entry for sharing cyber threat information with the Federal government will exponentially complicate efforts to ensure real-time sharing. **The Administration strongly supports the DHS portal established in S. 754 or Title II of H.R. 1560.**

3) **Defensive Measures**: The use of defensive measures without appropriate safeguards raises significant legal, policy, and diplomatic concerns and can have a direct deleterious impact on information systems and undermine cybersecurity. Moreover, certain provisions may prevent the application of laws such as State common law tort remedies. Legislation should not create a backdoor exception to 18 U.S.C. § 1030 by allowing "defensive measures" that access other computers without authorization. Language in S. 754, which prohibits the use of a countermeasure to provide unauthorized access to another entity's network, helps mitigate this concern. **As such, the Administration strongly prefers S. 754's definition of a defensive measure.**

a) *Distinguish Monitoring from Defensive Measures*: Both Title II of H.R. 1560 and S. 754 include monitoring activity within the definition of a defensive measure. The consequences of the overlapping terms in S. 754 and Title II of H.R. 1560 are unclear. However, a lack of clarity may create uncertainty as to whether an entity's activity to detect an intrusion is an authorized monitoring activity, which is covered by the bill's liability protections, or a defensive measure, which is not. The final bill should not