UPDATED

H.R. 1731, THE "NATIONAL CYBERSECURITY PROTECTION ADVANCEMENT ACT OF 2015" (NCPA ACT)

FACT SHEET

On April 13, 2015, Committee on Homeland Security Chairman Michael McCaul introduced H.R. 1731, the "National Cybersecurity Protection Advancement Act of 2015." The bill seeks to improve cyber information sharing with the Department of Homeland Security (DHS) and within the private sector – a top bipartisan legislative priority for the 114th Congress for President Obama, House and Senate Leadership, industry groups, and DHS. On April 14, 2015, the Committee approved H.R. 1731, as amended, by voice vote and it is expected to be considered by the House during the week of April 20, 2015. **Ranking Member Thompson and Cybersecurity, Infrastructure Protection and Security Technologies Ranking Member Cedric Richmond support this legislation.**

The NCPA Act largely reflects months of extensive bipartisan stakeholder outreach to representatives from critical infrastructure sectors, technology companies, privacy organizations, and DHS. The main provisions of NCPA Act, as reported by the Committee on Homeland Security, are as follows:

- Authorizes a non-Federal entity (e.g. company) to, *for a cybersecurity purpose*[1], voluntarily (1) share[2] information with DHS or another non-Federal entity about cyber threats (cyber threat indicators) and measures to defend their networks against such cyber threats (defensive measures); (2) monitor their own networks for cyber threats; and (3) operate measures to defend their networks against cyber threats.

- Requires both the non-Federal entity and DHS to take "reasonable efforts to remove information that can be used to identify specific persons and is reasonably believed at the time of sharing to be unrelated to a cybersecurity risk or incident."

- Confers liability protection against lawsuits to any non-Federal entity that shares cyber threat indicators or defensive measures or conducts authorized monitoring on their networks when acting in accordance with the requirements of the Act, so long as the non-Federal entity did not engage in "willful misconduct." Additionally, it specifically immunizes non-Federal entities for failing to act on information provided.

- Establishes substantial oversight and reporting requirements for the DHS Chief Privacy Officer, the DHS Chief Civil Rights and Civil Liberties Officer, the DHS Inspector General, and the Privacy and Civil Liberties Oversight Board.

[1] "Cybersecurity Purpose" is defined in the bill as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity risk or incident"; See Sec. 2(a).
[2] "Sharing" is defined in the bill as "providing, receiving, and disseminating"; See Sec. 2(a).

UPDATED

- Directs the streamlining of the National Protection and Programs Directorate (NPPD) into a new entity that will be known as "Cybersecurity and Infrastructure Protection," sets forth the leadership positions of that entity, and directs DHS to report on the feasibility of making it an operational component.

- Requires DHS to share information relating to cybersecurity risks and incidents with small and medium-sized businesses and to establish a cybersecurity awareness campaign to enhance education about cybersecurity issues among the public.

Committee Democrats support the goal of the NCPA Act – to enhance timely information sharing about hacks and other cyber threats to improve cybersecurity – and generally believe that the NCPA Act, if enacted, can help achieve this goal.

Some issues with the bill remain unresolved, however. Most notably, Committee Democrats support President Obama's tailored approach to addressing what some in industry have identified as a major barrier to the sharing cyber threat information – the risk that sharing such information would expose companies to legal liability. Unfortunately, the liability protection provision included in the NCPA Act does not provide straightforward protections and, instead, puts in place an unduly complicated structure that runs the risk of directly or inadvertently providing liability relief to companies that act negligently as lawsuits would only be allowed for "willful misconduct" and incentivizing companies to not act on timely cyber threat information, since it immunizes companies for failing to act on cyber information.

On April 21, 2015, the White House issued a Statement of Administration Policy expressing support for House passage of H.R. 1731 but expressing concern with the measure's "sweeping" liability protections that the White House fears "may weaken cybersecurity writ large." Unfortunately, the Rules Committee did not allow any of the seven amendments on the liability protection language to be considered.

Committee Democrats stand ready to refine the liability protection language as the legislation advances and support H.R. 1731, as it will bolster cybersecurity by ensuring that more Americans receive timely, actionable cyber threat information to secure their networks.