THE REPUBLICAN STUDY COMMITTEE
Rep. Bill Flores, Chairman
Freedom ★ Liberty ★ Opportunity ★ Security
202.225.6105
rsc.flores.house.gov

H.R. 1731— National Cybersecurity Protection Advancement Act of 2015 (Rep. McCaul, R-TX)

CONTACT: NICHOLAS RODMAN, NICHOLAS.RODMAN@MAIL.HOUSE.GOV, 6-8576

FLOOR SCHEDULE: SCHEDULED FOR CONSIDERATION ON APRIL 23, 2015 UNDER A CLOSED RULE THAT PROVIDES FOR ONE HOUR OF DEBATE

TOPLINE SUMMARY: H.R. 1731 would amend the Homeland Security Act of 2002 by clarifying the role of the Department of Homeland Security's National Cybersecurity and Communications Integration Center in sharing cyber threat information with other federal and non-federal entities. Similar to H.R. 1560, the bill would also extend civil and criminal liability protection to cybersecurity providers and other entities that monitor, share, or use cyber threat information.

CONSERVATIVE CONCERNS: Some conservative shave deemed the government's efforts to maintain a balance between national security and privacy as unsatisfactory, due in part to concerns over the cost of these cybersecurity efforts, governmental duplication, and the erosion of privacy rights. H.R. 1731's liability protection provisions have also been an issue of concern. Other conservatives believe that the threat posed by cyberattacks on the U.S. economy, infrastructure, and overall national security remains an ever increasing danger and must be addressed through increased information sharing and liability protection.

- **Expand the Federal Government?** No.
- **Encroach into State or Local Authority?** No.
- **Delegate Any Legislative Authority to the Executive Branch?** No.
- **Contain Earmarks/Limited Tax Benefits/Limited Tariff Benefits?** No.

COST: The Congressional Budget Office (CBO) estimates that enacting H.R. 1731 would cost approximately $20 million over the 2016-2020 period, assuming appropriation of the estimated amounts.

H.R. 1731 would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), by extending civil and criminal liability protection to cybersecurity providers and other entities that monitor, share, or use information on cyber threats. Doing so would prevent public and private entities from seeking compensation for damages from those protected entities for sharing or using cybersecurity information.

DETAILED SUMMARY AND ANALYSIS: Section 2 of H.R. 1731 would amend the Homeland Security Act of 2002 by defining the term "cyber threat indicator" as technical information that is necessary to describe or identify a method for probing, monitoring, maintaining, or establishing network awareness of an information system for the purpose of discerning technical vulnerabilities. The section further defines the terms "cybersecurity purpose", "defensive measure", "network awareness", "private entity", "security control", and "sharing".

Section 3 codifies the role of the National Cybersecurity and Communications Integration Center (NCCIC) by designating the agency as the "'the lead federal civilian interface" for the multi-directional and cross-sector sharing of information related to cybersecurity risks, incidents, analysis, and warnings for federal and non-federal entities. It also clarifies that the NCCIC would coordinate the sharing of information related to cyber

threat indicators and defensive measures, and would conduct integration and analysis, including cross-sector integration and analysis, of cyber threat indicators, defensive measures, and cybersecurity risks. The center is directed to share cyber threat indicators with federal and non-federal entities, across sectors of critical infrastructure and with state and major urban area fusion centers. The center is mandated to promptly notify the Secretary of Homeland Security and Congress of any significant violations of the policies and procedures specified in the bill, and to promptly notify non-federal entities that have shared cyber threat indicators or defensive measures that are known or determined to be in error or in contravention of the bill's requirements. The section expands the center's composition to include an entity to collaborate with state and local governments; the U.S. Computer Emergency Readiness Team to coordinate information related to cybersecurity risks and incidents and provide technical assistance; the Industrial Control System Cyber Emergency Response Team to coordinate with industrial control systems owners and operators; and the National Coordinating Center for Communications to coordinate the resilience and recovery of national security emergency communications.

Section 3 requires the Under Secretary of Homeland Security for Cybersecurity and Infrastructure Protection to develop an automated capability for the timely sharing of cyber threat indicators and defensive measures. The NCCIC is additionally mandated to develop the capability to share cyber threat indicators and defensive measures with each federal entity designated as the "Sector Specific Agency" for each critical infrastructure sector in as close to real time as practicable. The section further directs the Under Secretary to submit a biannual report to Congress on the progress of developing this capability. The center is authorized to enter into a voluntary information sharing relationship with any consenting non-federal entity for the sharing of cyber threat indicators and defensive measures for cybersecurity purposes. The center could terminate a voluntary information sharing relationship if it determines that the non-federal entity with which the center has entered into a relationship has, after multiple notices, repeatedly violated the bill's provisions. The section further authorizes a non-federal entity to share cyber threat indicators or defensive measures obtained from its own information system or, with written consent, from an information system of another federal or non-federal entity, with another private or state entity as well as the NCCIC for cybersecurity purposes, but must take reasonable efforts to remove information that could be used to identify specific persons unrelated to a cybersecurity threat.

Section 3 would also direct the Under Secretary of Homeland Security for Cybersecurity and Infrastructure Protection in coordination with the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties at the Department of Homeland Security to establish and annually review policies and procedures for the Department that govern the use and disclosure of cyber threat indicators and information. Under the privacy subsection, the Department's Office of the Inspector General (DHS OIG) is mandated to submit a report to Congress within two years of the bill's enactment and periodically thereafter that includes a review of the type of information shared with NCCIC, the use of any information and actions taken by the center, and the impact of sharing of such information on privacy and civil liberties.

A non-federal entity that shares cybersecurity information with the NCCIC, or another non-federal entity is permitted to use or disclose those cyber threat indicators and defensive measures solely for cybersecurity purposes, but must remove information that could be used to identify specific persons unrelated to a cybersecurity threat. A non-federal entity is also required to implement and utilize a security control to protect against unauthorized access to cyber threat indicators or defensive measures. Similar requirements would additionally apply to federal entities.

Section 3 would grant liability protection to any non-federal entity that conducts network awareness or shares cyber threat indicators or defensive measures, for cybersecurity purposes, in accordance with the bill, and provides liability protection for a non-federal entity that fails to act upon shared cyber threat indicators or defensive measures, unless willful misconduct has occurred. If a department or agency of the federal government intentionally or willfully violates the bill's restrictions, the federal government would then be liable to a person injured by such violation.

Section 5 of the bill would designate the National Protection and Programs Directorate of the Department of Homeland Security as the "Cybersecurity and Infrastructure Protection Directorate" and requires a report on the feasibility of making the Cybersecurity and Communications Office an operational component of the Department of Homeland Security.

Section 6 would require the Secretary of Homeland Security to update, maintain, and exercise the Cyber Incident Annex to the Department's National Response Framework.

Section 7 would require the NCCIC to assess the effects of cyber incidents on public safety communications, and requires the Under Secretary of Homeland Security for Cybersecurity and Infrastructure Protection to develop and implement a cybersecurity awareness campaign regarding cybersecurity risks and voluntary best practices for mitigating and responding to cybersecurity risks.

Section 10 would mandate that the Government Accountability Office (GAO) submit a report to Congress assessing the bill's implementation no later than two years after its enactment.

Section 13 would specify that the bill would not grant the Secretary of Homeland Security any authority to promulgate regulations or set standards relating to the cybersecurity of private entities, except for state, local, or tribal governments.

Section 14 would mandate that all reporting requirement in the bill are removed 7 years after the bill's enactment.

Section 15 would clarify that no new funds are authorized to be appropriated to carry out the bill.

According to the House Committee on Homeland Security, H.R. 1731 ensures that "the sharing of cyber threats is transparent and timely," while bolstering "the robust privacy protections already in place at DHS without risking [the] exposure of personal data". The bill would seek to improve how the Department of Homeland Security defends the federal government and non-federal or private entities against the growing threat of cyber espionage and cyber-attacks through voluntary information sharing. At the same time, the bill would seek to maintain and strengthen privacy protections by restricting and prohibiting the release of private information unrelated to cyber threats.

The House Report (H. Rept. 114-83) accompanying H.R. 1731 can be found here. A section by section, and bill summary from the House Committee on Homeland Security can be found here. A Congressional Research Service report on Cybersecurity and Information Sharing comparing H.R. 1560 with H.R. 1731 can be found here. A Heritage Foundation research paper on the cybersecurity legislation can be found here.

OUTSIDE ORGANIZATIONS:

- **In Support:**
  American Chemistry Council (ACC)
  AT&T
  BSA / The Software Alliance
  Depository Trust & Clearing Corporation (DTCC)
  Energy and Utilities Sector - Joint Trade Associations
  Financial Services Sector - Joint Trade Associations
  Information Technology Industry Council (ITI)
  Oracle

Protecting America's Cybersecurity Networks Coalition including the American Petroleum Institute, National Association of Manufacturers, and the Federation of American Hospitals
Telecommunications Sector including the National Cable and Telecommunications Association
Verizon
U.S. Chamber of Commerce
More letters of support can be found here.

- **In Opposition:**
  Generation Opportunity
  FreedomWorks
  Technologists and Academics Letter

AMENDMENTS MADE IN ORDER:

- McCaul #34 (Manager's Amendment) would make technical corrections and further clarifies that nothing in the bill would be construed to permit price fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.
- Mulvaney #38 would sunset the provisions of the bill after 7 years. According to the amendment's sponsor, the provision "gives a future Congress the opportunity to assess whether the balance we have struck between security and liberty is still the right one."
- Castro #6 would make self-assessment tools available to small and medium-sized businesses to determine their level of cyber security readiness.
- Castro #7 would establish the National Cybersecurity Preparedness Consortium, which would provide training to state and local first responders and officials specifically for preparing and responding to cyber-attacks, and would consist of academic, nonprofit, and government partners that develop, update, and deliver cybersecurity training in support of homeland security.
- Hahn #39 would require the Secretary of Homeland Security to submit to Congress a report on cybersecurity vulnerabilities for the ten United States ports that the Secretary determines are at greatest risk of a cybersecurity incident and provide recommendations to mitigate such vulnerabilities, not later than 180 days after the bill's enactment.
- Hurd #35 would authorize the Einstein 3A (E3A) intrusion detection program by allowing the Secretary of Homeland Security to deploy and operate capabilities to protect federal agency information and information systems, including technologies to continuously diagnose, detect, prevent, and mitigate against cybersecurity risks. The amendment offers states that no cause of action shall lie against a private entity for assistance provided to the Secretary in accordance with the bill.
- Jackson Lee #12 would require a GAO report on the impact on privacy and civil liberties limited to the work of the National Cybersecurity and Communications Integration Center.
- Jackson Lee #16 would require federal agencies related to the cybersecurity of the private sector to remain current on industrial control system innovation; industry adoption of new technologies, and industry best practices.
- Jackson Lee #17 would require the Secretary of Homeland Security to submit to Congress a report on how best to align federally-funded cybersecurity research and development activities with private sector efforts to protect privacy and civil liberties while assuring security and resilience of the Nation's critical infrastructure.
- Katko #33 would clarify and define the term "incident" in the bill to mean an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.
- Langevin #21 would clarify and define the term "cyber security risk" to mean threats to and vulnerabilities of information or information systems and any related consequences caused by or

resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

COMMITTEE ACTION: This bill was introduced on April 13, 2015 and was referred to the House Committee on Homeland Security, which ordered it to be reported (amended) by voice vote.

ADMINISTRATION POSITION: A statement of administration position can be found here. While largely in support, the administration has concerns "that the bill's authorization to operate defensive measures is not adequately tailored" regarding the use of defensive measures without appropriate safeguards.

CONSTITUTIONAL AUTHORITY: Congress has the power to enact this legislation pursuant to the following: Article I, Section 8, Clause-To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof.

NOTE*: RSC Legislative Bulletins are for informational purposes only and should not be taken as statements of support or opposition from the Republican Study Committee.*

###