never complained and always carried himself with a dignity that defined who he was. He leaves behind an enormous legacy and some big shoes to fill in the union. I extend my deepest sympathies to Babe's family, friends, and Union family. I know he is deeply missed by all.

STOP UNDERRIDES ACT OF 2017

HON. STEVE COHEN

OF TENNESSEE

IN THE HOUSE OF REPRESENTATIVES

Tuesday, December 12, 2017

Mr. COHEN. Mr. Speaker, I rise in support of the Stop Underrides Act, a bipartisan, bicameral bill I introduced earlier today along with my colleague on the Transportation & Infrastructure Committee, Rep. DESAULNIER from California, and in the Senate, Senators GILLIBRAND and RUBIO, to prevent deadly truck underride crashes.

An underride crash is when a car slides under the body of a large truck, such as a semi-trailer, during an accident. In these instances, the safety features of passenger vehicles are not able to prevent passenger compartment intrusion and often result in severe or fatal injuries even at low speeds.

Too many lives have been lost or forever altered by these preventable crashes and the time has come for Congress to act.

The Stop Underrides Act does just that—lays out a path to bring an end to these terrible and all too often fatal accidents by requiring all large truck trailers to have front, side, and rear underride guards.

These guards, if installed would have likely prevented the death of Michael Higginbotham, who was killed in an underride crash in Memphis and whose parents, Randy and Laurie Higginbotham, have inspired me to take action on this long overdue issue.

It's simple. This legislation will save lives, it's the right thing to do, and that is the bottom line.

This is common sense legislation and I urge my colleagues to support the passage of the Stop Underrides Act.

PERSONAL EXPLANATION

HON. JOHN B. LARSON

OF CONNECTICUT

IN THE HOUSE OF REPRESENTATIVES

Tuesday, December 12, 2017

Mr. LARSON of Connecticut. Mr. Speaker, on December 7, 2017 I missed Roll Call vote 671. Had I been present, I would have voted yea.

RECOGNIZING THE CONTRIBUTIONS OF STANTON GILDENHORN ON THE OCCASION OF HIS 75TH BIRTHDAY

HON. JAMIE RASKIN

OF MARYLAND

IN THE HOUSE OF REPRESENTATIVES

Tuesday, December 12, 2017

Mr. RASKIN. Mr. Speaker, I rise today to recognize the great contributions that have been rendered to our country and to my home state of Maryland by my constituent and wonderful friend, Stanton Gildenhorn. I offer these remarks just a few days ahead of Stan's 75th birthday next week.

Stan is a well-known public servant, politico, and television personality in our community. He got his start as the youngest staffer in President John F. Kennedy's White House and later worked for the U.S. Securities and Exchange Commission.

Stan earned a J.D. from the George Washington University School of Law and worked as an attorney in private practice for many years, including in Rockville. He also put his superior legal skills to good use to benefit our community by working at non-profit organizations like the Montgomery County Humane Society and serving as both the Chairman and Counsel for the Montgomery County Democratic Central Committee.

A passionate political thinker and strategist, Stan has managed or worked on dozens of campaigns in the last 40 years, at nearly every level of government, and chaired the Montgomery County Charter Review Commission. He was a fixture on national and local television shows for decades, and continues to offer valuable and incisive political commentary today.

I am honored to recognize the important contributions of my constituent, Mr. Stanton Gildenhorn today and hope this chamber will join me in wishing him a happy 75th birthday.

HONORING JACKIE GILLAN, PRESIDENT OF ADVOCATES FOR HIGHWAY AND AUTO SAFETY

HON. JANICE D. SCHAKOWSKY

OF ILLINOIS

IN THE HOUSE OF REPRESENTATIVES

Tuesday, December 12, 2017

Ms. SCHAKOWSKY. Mr. Speaker, I rise to celebrate the career of Jackie Gillan, President of Advocates for Highway and Auto Safety. Jackie will soon be retiring after nearly 30 years with Advocates.

For decades, Jackie has been at the forefront of transportation safety—in and out of government. Her record of public service is impressive. She served as a staffer at the U.S. Department of Transportation during the Carter Administration and in the U.S. Senate. She has also worked at state transportation agencies in New Jersey, Ohio, and California.

I know Jackie from her post-government career as a champion for consumer safety. She joined Advocates as a board member in 1989. She became Vice President a year later and President in 2011.

Under her leadership, Advocates has worked effectively at the federal and state levels to improve child safety; strengthen laws against impaired driving; require seatbelts, child restraints, and motorcycle helmets; establish teen driver programs; and increase funding for highway and auto safety. In 2002, two-year-old Cameron Gulbransen was killed in a tragic back-over accident. With Jackie's help, I passed a bill in Cameron's memory to require back-up cameras in passenger vehicles. The fight did not stop there though. We fought for years afterward to implement the law until the National Highway Traffic Safety Administration finalized a rule in 2014. Thanks to Jackie's tireless efforts, back-up cameras are now standard in Model Year 2018 passenger vehicles.

This year, we have been working together to pass the HOT CARS Act, which would help prevent child heatstroke deaths by requiring rear seat reminders. Jackie has been an ally in numerous other efforts as well, from limiting the sale of cars under open recall to ensuring the safe deployment of autonomous vehicles.

Jackie leaves her current role with an impressive legacy of crashes prevented, injuries averted, and lives saved. But I don't expect Jackie to disappear into retirement. As she moves from President to President Emeritus of Advocates for Highway and Auto Safety, I am confident that she will continue to be a safety champion. And whether they know it or not, everyone on the road today owes a little bit of gratitude to Jackie Gillan.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY ACT OF 2017

SPEECH OF

HON. SHEILA JACKSON LEE

OF TEXAS

IN THE HOUSE OF REPRESENTATIVES

Monday, December 11, 2017

Ms. JACKSON LEE. Mr. Speaker, I rise to speak in support of H.R. 3359, the Cybersecurity and Infrastructure Security Agency Act of 2017.

I thank Chairman MCCAUL for introducing this important piece of legislation that addresses the cybersecurity needs of our nation.

H.R. 3359, amends the Homeland Security Act of 2002 to redesignate the Department of Homeland Security's (DHS's) National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency (CISA).

Under its new designation the CISA would be headed by a Director of National Cybersecurity and Infrastructure Security, who will be responsible for leading national efforts to protect and enhance the security and resilience of U.S. cybersecurity, emergency communications, and critical infrastructure.

CISA will be composed of DHS components reorganized as: the Cybersecurity Division; the Infrastructure Security Division; and the Emergency Communications Division, which was previously the Office for Emergency Communications.

The agency will also have its own privacy officer to ensure compliance with relevant federal laws.

CISA must carry out DHS's responsibilities concerning chemical facilities antiterrorism standards.

The bill requires DHS to:

develop, implement, and continually review a maritime cybersecurity risk assessment model to evaluate current and future cybersecurity risks;

seek input from at least one information sharing and analysis organization representing maritime interests in the National Cybersecurity and Communications Integration Center;

establish voluntary reporting guidelines for maritime-related cybersecurity risks and incidents;

request that the National Maritime Security Advisory Committee report and make recommendations to DHS about methods to enhance cybersecurity and information sharing

among security stakeholders from federal, state, local, and tribal governments; public safety and emergency response agencies; law enforcement and security organizations; maritime industry participants; port owners and operators; and maritime terminal owners and operators; and

ensure that maritime security risk assessments include cybersecurity risks to ports and the maritime border of the United States.

As with other threats that this nation has faced and overcome, we must create the resources and the institutional responses to protect our nation against cyber threats while preserving our liberties and freedoms.

We cannot accomplish this task without the full cooperation and support of the private sector, computing research community and academia.

Earlier this Congress, I introduced H.R. 3202, the Cyber Vulnerability Disclosure Reporting Act, which was passed by the full Homeland Security Committee.

H.R. 3202 requires the Secretary of Homeland Security to submit a report on the policies and procedures developed for coordinating cyber vulnerability disclosures.

The report will include an annex with information on instances in which cyber security vulnerability disclosure policies and procedures were used to disclose details on identified weaknesses in computing systems that or digital devices at risk.

The report will provide information on the degree to which the information provided by DHS was used by industry and other stakeholders.

The reason that I worked to bring this bill before the committee is the problem often referred to as a ''Zero Day Event,'' which describes the situation that network security professionals may find themselves when a previously unknown error in computing code is exploited by a cybercriminal or terrorist.

I am pleased that the Committee on Homeland Security passed H.R. 3202 to address the need to support information sharing regarding threats to computing networks.

I look forward to the Full House consideration of H.R. 3202.

In the first few weeks of this Congress I introduced a number of measures on the topic of cybersecurity to address gaps in our nation's cyber defensive posture:

SCOUTS Act—H.R. 940;

CAPITALS Act—H.R. 54;

SAFETI Act—H.R. 950;

Terrorism Prevention and Critical Infrastructure—H.R. 945; and

Cybersecurity and Federal Workforce Enhancement Act—H.R. 935.

H.R. H.R. 940, the ''Securing Communications of Utilities from Terrorist Threats'' or the ''SCOUTS Act,'' directs the Secretary of Homeland Security, in coordination with the sector-specific agencies, to work with critical infrastructure owners and operators and State, local, tribal, and territorial entities to seek voluntary participation on ways that DHS can best defend against and recover from terrorist attacks that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof.

H.R. 940, is relevant to today's hearing because it addresses the need for a two way communication process that enables private sector participants in information sharing arrangements with DHS to communicate their views on the effectiveness of the information provided; the method of information sharing; and their particular needs as time passes.

Specifically the bill establishes voluntary listening opportunities for sector specific entities to communicate their challenges regarding cybersecurity, including what needs they may have for critical infrastructure protection; and how DHS is helping or not helping to meet those needs.

The Society of Maintenance and Reliability Professionals have endorsed H.R. 940, and input on the legislation included the Edison Electric Institute, an electric utility association.

H.R. 54, the Department of Homeland Security's Cybersecurity Asset Protection of Infrastructure under Terrorist Attack Logistical Structure or CAPITALS Act, which directs the Department of Homeland Security (DHS) to produce a report to Congress regarding the feasibility of establishing a DHS Civilian Cyber Defense National Resource.

H.R. 950, requires a report and assessment regarding Department of Homeland Security's response to terrorist threats to Federal elections. The Comptroller General of the United States is directed to conduct an assessment of the effectiveness of Department of Homeland Security actions to protect election systems from cyber-attacks and to make recommendations for improvements to the actions taken by DHS if determined appropriate.

H.R. 935, The ''Cybersecurity and Federal Workforce Enhancement Act'' identifies and trains people already in the workforce who can obtain the skills to address our nation's deficit in the number of workers and positions available for those with needed skills.

H.R. 940, the ''Securing Communications of Utilities from Terrorist Threats'' or the ''SCOUTS Act,'' is the relevant to today's hearing because this bill focuses on the communications sent by DHS to sector specific entities and the ability of these entities to communicate to the agencies their perspective on the usefulness of the information; the form of communication that would be most helpful; and requires a report to Congress by DHS on the views of critical infrastructure owners and operators on the information sharing process related to cybersecurity.

Each of these bills will build upon an aggressive approach for securing cyber technology to manage critical infrastructure, chemical facilities, and port operations, ranging from communication and navigation to engineering, safety, and pipelines, that are critical to protect our nation's interest.

Over the past year, Russian actors' targeted U.S. election infrastructure, hackers escalated efforts to breach the domestic energy sector, and WannaCry and NotPetya ransomware wreaked havoc on public and private infrastructure around the world.

According to Symantec, a leading provider of cybersecurity solutions, said that ''The world of cyber espionage experienced a notable shift towards more overt activity, designed to destabilize and disrupt targeted organizations and countries.''

As cyber threats continue to evolve and become more sophisticated, so must U.S. efforts to confront them.

The Department of Homeland Security, through the National Protection and Programs Directorate (NPPD), plays a central role in the federal government's cybersecurity apparatus and in coordinating federal efforts to secure critical infrastructure.

DHS is charged with coordinating agency efforts to secure the (dot).gov Domain, while also serving as the hub for cybersecurity information sharing between and among the private sector and federal government.

It is my hope that as this Congress moves forward that we will seek out the best ways to bring the brightest and most qualified people into the government as cybersecurity professionals.