THE REPUBLICAN STUDY COMMITTEE
Rep. Rob Woodall, Chairman
202.225.4272
rsc.woodall.house.gov

Legislative Bulletin……..……..……December 11, 2014

Contents:

Concur in the Senate Amendment to H.R. 2952 — Cybersecurity Workforce Assessment Act (Rep. Meehan, R-PA)

Order of Business: The bill is scheduled to be considered on December 11, 2014, under a motion to suspend the rules and pass the bill, which requires a two-thirds majority for passage.

Summary: H.R. 2952 would rename the bill as the Cybersecurity Workforce Assessment Act. The bill would direct the Secretary of Homeland Security to transmit to Congress within 180 days of the bill's enactment, and annually for 3 years, a cybersecurity assessment of the Department including:

- An assessment of the readiness and capacity of the workforce of the Department to meet its cybersecurity mission;
- Information on where cybersecurity workforce positions are located within the Department;
- Information on which cybersecurity positions are performed by permanent full-time equivalent employees, independent contractors, and individuals employed by other Federal agencies, including the National Security Agency; and
- Information on the percentage of individuals within each cybersecurity category and specialty area who received essential training.

The Secretary of Homeland Security is directed to submit to Congress a comprehensive workforce strategy to enhance the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department. The Secretary shall submit to Congress a report on the feasibility, cost, and benefits of establishing a Cybersecurity Fellowship program to offer a tuition payment plan for individuals pursuing undergraduate and doctoral degrees who agree to work for the Department for an agreed-upon period of time.

Additional Information: The RSC's legislative bulletin for the House-passed H.R. 2952 can be found here. The report (H. Rept. 113-324) accompanying H. R. 2952 can be found here.

Committee Action: The bill was introduced on August 1, 2013 and was referred to the House Committee on Homeland Security. On October 29, 2013, H. R. 2952 was marked-up and ordered to be reported (amended) by voice vote. On January 9, 2014, the bill was reported (amended) by the House Committee on Homeland Security. On July 28, 2014, the bill was passed by the House under a motion to suspend the rules, as amended, and agreed to by voice vote.

Administration Position: No Statement of Administration Policy is available.

Cost to Taxpayers: The Congressional Budget Office (CBO) estimates that implementing H. R. 2952 would have discretionary costs totaling less than $500,000 in each of fiscal years 2014 and 2015. Enacting the legislation would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply. CBO estimates the Department of Homeland Security and the Government Accountability Office reports required by H. R. 2952 would cost less than $500,000 annually in 2014 and 2015, assuming availability of appropriated funds. The CBO estimate for the House-passed H.R. 2952 can be found here.

Does the Bill Expand the Size and Scope of the Federal Government?: No.

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates?: The House-passed H. R. 2952 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments.

Constitutional Authority: Congress has the power to enact this legislation pursuant to the following: 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.

RSC Staff Contact: Nicholas Rodman, nicholas.rodman@mail.house.gov, (202) 226-8576

***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.*

Concur in the Senate Amendment to H.R. 4007 — Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (Rep. Meehan, R-PA)

Order of Business: The bill is scheduled to be considered on December 11, 2014, under a motion to suspend the rules and pass the bill, which requires a two-thirds majority for passage.

Summary: H.R. 4007 would amend the Homeland Security Act of 2002 by requiring the Department of Homeland Security to establish a Chemical Facility Anti-Terrorism Standards Program. The bill would direct the Secretary of Homeland Security to identify chemical facilities of interest and covered chemical facilities. The Secretary is authorized to require chemical facilities of interest to submit a Top-Screen. The bill authorizes the Secretary to require covered facilities to submit to the Department of Homeland Security security vulnerability assessments, and to develop, submit, and implement site security plans.

A facility, in developing a site security plan, shall include security measures that appropriately address the security vulnerability assessment and the risk-based performance standards for security for the facility. The bill would outline the process for the Department's review of site security plans and improve the efficiency of the site security plan approval process by allowing facilities to use an alternative security program. The Secretary of Homeland Security is required to evaluate and approve site security plans. In approving or disapproving a site security plan under this subsection, the Secretary shall employ the risk assessment policies and procedures.

The Secretary of Homeland Security may approve an alternative security program established by a private sector entity or a Federal, State, or local authority, or under other applicable laws, if the Secretary determines that the requirements of the program meet the requirements of the risk-based performance standards listed in the bill. In the case of a covered chemical facility for which the Secretary approved a site security plan before the date of the bill's enactment, the Secretary may not require the facility to resubmit the site security plan solely by reason of the enactment.

The bill also creates a new expedited approval program through which tier 3 and 4 facilities may develop and submit a site security plan for expedited approval. It requires that the Secretary first issue prescriptive guidance for such facilities to meet the risk-based performance standards and outlines how facilities may certify that deviations from the guidance meet or exceed the prescriptive standards.

The Secretary is required to conduct audits or inspections of covered chemical facilities and allow nongovernmental personnel to conduct audits or inspections on behalf of the Department in order to address the existing backlog. The bill also requires the Secretary to establish a Personnel Surety Program that ensures individuals with access to covered chemical facilities are vetted against the Terrorist Screening Database.

The Department of Homeland Security is required to communicate with state and local officials, as well as other Federal agencies and industry associations, to identify chemical facilities of interest, which will help to ensure that outlier facilities are known to the Department. The bill further ensures that the Department is taking into account all relevant risk information when developing its risk assessment standards and corresponding tiering methodology. It also requires that the Secretary document the basis for each change in a covered chemical facility's tier. It also requires the Secretary to provide a biannual report to Congress detailing specific metrics on the program's performance in order to aid Congressional evaluation and oversight of the program.

- Section 2103 ensures that sensitive security information is protected, and shared with first responders in a secure, responsible manner in order to prevent loss of life and property. It ensures that sensitive information regarding a facility, where disclosure could present a potential risk, developed under this Act shall not be made available for public disclosure.

- Section 2104 specifies penalties for noncompliance and sets the parameters of civil liability.

- Section 2105 clarifies whistleblower protections available to chemical facility employees and contractors, and requires these protections be publicly disclosed and advertised.

- Section 2107 specifies that the Department can continue to follow previously-issued regulations, and does not need to undertake a new rulemaking.

- Section 2109 directs the Secretary to develop an implementation plan for outreach to chemical facilities of interest in order to minimize the number of outliers.

Additional Information: The RSC's legislative bulletin on the House-passed H.R. 4007 can be found here. The Senate report (S. Rept. 113- 263) accompanying H.R. 4007 can be found here. The House report (H. Rept. 113-491) accompanying H.R. 4007 can be found here. A Congressional Research Service report on H.R. 4007 can be found here. A letter of support from several associations, including the American Chemistry Council, the U.S. Chamber of Commerce, and the National Association of Manufacturers in support of H.R. 4007 can be found here.

Committee Action: The bill was introduced on February 6, 2014 and was referred to the House Committee on Homeland Security and the House Committee on Energy and Commerce. The bill was reported out and amended by the House Committee on Homeland Security on June 23, 2014. On July 8, 2014, the bill was passed by the House under a motion to suspend the rules, as amended, and agreed to by voice vote.

Administration Position: No Statement of Administration Policy is available.

Cost to Taxpayers: H.R. 4007 would authorize CFATS for an additional four years and would create an expedited review procedure for facilities in the lower risk tiers of the CFATS program. Based on amounts requested for the CFATS in fiscal year 2015 as well as information from DHS, the Congressional Budget Office (CBO) estimates that continued implementation of CFATS would require appropriations of $87 million in 2015 and slightly higher amounts in fiscal years 2016 through 2018 after accounting for the effects of inflation. Assuming appropriation of the estimated amounts, CBO estimates that implementing H.R. 4007 would result in outlays of $349 million over the 2015-2019 period.

Enacting H.R. 4007 could result in the collection of additional civil penalties, which are recorded as revenues and deposited in the Treasury; therefore, pay-as-you-go procedures apply. However, CBO estimates that such collections would be insignificant. Enacting the bill would not affect direct spending.

The CBO estimate ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on July 30, 2014 can be found here.

Does the Bill Expand the Size and Scope of the Federal Government?: No.

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates?: H.R. 4007 would extend intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), on owners and operators of public and private facilities where certain chemicals are present. Current law requires owners and operators to assess the vulnerability of their facilities to a terrorist incident and to prepare and implement facility security plans. This bill would extend, for four years, the authority of DHS to regulate those facilities through minimum standards designed to protect facilities from acts of terrorism and other security risks. The requirement to meet those standards would be a mandate on public and private entities. The bill would impose an additional mandate on public and private employers by prohibiting them from discharging or discriminating against employees who report security problems at a covered chemical facility.

Information from the Department of Homeland Security indicates that owners and operators of chemical facilities already meet the existing security standards and that they would only need to make small changes to administrative procedures to comply with the new whistleblower protections for their employees. Therefore, CBO estimates that the aggregate additional costs of complying with the mandates would be small and would fall below the annual thresholds established in UMRA for intergovernmental and private-sector mandates ($76 million and $152 million, respectively, in 2014, adjusted annually for inflation).

Constitutional Authority: Congress has the power to enact this legislation pursuant to the following: Article I, section 8, clause 1; and Article I, section 8, clause 18 of the Constitution of the United States.

RSC Staff Contact: Nicholas Rodman, nicholas.rodman@mail.house.gov, (202) 226-8576

***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.*

S. 2519 - National Cybersecurity Protection Act of 2014
(*Sen. Carper*, D-DE)

Order of Business: The bill is scheduled to be considered on December 11, 2014, under a motion to suspend the rules and pass the bill, which requires a two-thirds majority for passage.

Summary: S. 2519 would amend the Homeland Security Act of 2002 by authorizing the establishment of a National Cybersecurity and Communications Integration Center to carry out the responsibilities of the Department of Homeland Security Under Secretary responsible for

overseeing critical infrastructure protection, cybersecurity, and related Homeland Security programs. The cybersecurity functions of the center shall include:

- Being a 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;

- Providing shared situational awareness to enable real-time operations;

- Sharing cybersecurity threat, vulnerability, impact and incident information and analysis by and among Federal, State, and local government entities and private sectors;

- Coordinating cybersecurity information sharing throughout the Federal government;

- Conducting analysis of cybersecurity risks and incidents; providing technical assistance to Federal and non-Federal entities, upon request, with respect to threats, attribution, vulnerability mitigation, and incident response and remediation, and providing recommendations on security and resilience.

The center is to be composed, at the discretion of the Under Secretary responsible for overseeing critical infrastructure protection and cybersecurity of personnel from Federal agencies, including civilian and law enforcement agencies and the intelligence community, and representatives from state and local governments and other non-Federal entities.

The Secretary is required to submit an annual report one year after the date of enactment of the bill and for each of the next three years thereafter, including an analysis of the performance of the operations center in carrying out the functions that would include: information on the composition of the center; and information on the policies and procedures established by the center to safeguard privacy and civil liberties.

The Government Accountability Office is also required to submit to Congress, a report one year after the date of enactment of the bill on the effectiveness of the operations center.

The bill would make clear that it is within the discretion of the Under Secretary whether to include in the center, or provide information and assistance to, governmental or private entities.

Additional Information: The Senate report (S. Rept. 113-240) accompanying S. 2519 can be found here.

Committee Action: The bill was introduced on June 24, 2014, and was referred to the Senate Committee on Homeland Security and Government Affairs.

Administration Position: No Statement of Administration Policy is available.

Cost to Taxpayers: S. 2519 would codify the National Cybersecurity and Communications Integration Center (NCCIC)'s current role in protecting federal civilian agencies in cyberspace,

sharing information on cybersecurity threats with Department of Homeland Security partners, and analyzing cybersecurity risks and incidents. The Congressional Budget Office (CBO) estimates that implementing the legislation would not result in a significant cost.

Enacting S. 2519 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply. The CBO estimate can be found here.

Does the Bill Expand the Size and Scope of the Federal Government?: No.

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates?: S. 2519 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would impose no costs on state, local, or tribal governments.

Constitutional Authority: Legislation introduced in the Senate does not require a constitutional authority statement.

RSC Staff Contact: Nicholas Rodman, nicholas.rodman@mail.house.gov, (202) 226-8576

***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.*