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

Legislative Bulletin…….……..……July 28, 2014

Contents:

H. R. 3202 – The Essential Transportation Worker Identification Credential Assessment Act
(*Rep. Jackson Lee*, D-TX)

Order of Business: The bill is scheduled to be considered on July 28, 2014, under a motion to suspend the rules and pass the bill, which requires a two-thirds majority for passage.

Background: According to the report accompanying H. R. 3202, the Transportation Worker Identification Credential (TWIC) program was established by the Maritime Transportation Security Act of 2002 to ensure secure access control to port facilities and vessels by capturing biometric information of all transportation workers with unescorted access to secure areas. The report (H. Rept. 113- 528) accompanying H. R. 3202 can be found here.

Summary: H. R. 3202 requires the Secretary of Homeland Security to prepare a comprehensive security assessment of the Transportation Worker Identification Credential (TWIC) program. Section 2 of the legislation directs the Secretary of Homeland Security to submit to Congress and to the Comptroller General of the United States a comprehensive assessment of the effectiveness of the transportation security card program at enhancing security and reducing security risks for facilities and vessels. The assessment would include:

- An evaluation of the extent to which the program, as implemented, addresses known or likely security risks in the maritime environment;
- An evaluation of the extent to which deficiencies identified by the Comptroller General have been addressed; and
- A cost-benefit analysis of the program, as implemented.

H. R. 3202 also directs the Secretary of Homeland Security to submit a corrective action plan that responds to the findings of the cost-benefit analysis of the transportation security card program, including an implementation plan with benchmarks, programmatic reforms, revisions to regulations, or proposals for legislation. The Comptroller General of the United States is also directed to review the implementation plan and to determine the extent to which certain Government Accountability Office (GAO) recommendations have been implemented.

H. R. 3202 prohibits the Secretary of Homeland Security from issuing a final rule requiring the use of transportation security card readers until:

- The Comptroller General informs Congress that the submission is responsive to the GAO recommendations; and

- The Secretary of Homeland Security issues an updated list of transportation security card readers that are compatible with active transportation security cards.

Paragraph 1 of the bill would not apply to any final rule issued pursuant to the notice of proposed rulemaking on Transportation Worker Identification Credential (TWIC)-Reader Requirements published by the Coast Guard on March 22, 2013. The Comptroller General of the United States is also directed to report to Congress regarding implementation of the Department of Homeland Security corrective action plan.

Section 3 of the bill would mandate that no additional funds are authorized to be appropriated to carry out H. R. 3202.

Committee Action: The bill was introduced on September 27, 2013, and was referred to the House Committee on Homeland Security. On June 11, 2014, the bill was marked-up by the House Committee on Homeland Security, and was ordered to be reported by voice vote. On July 17, 2014, the bill was reported (amended) by the committee.

Administration Position: No Statement of Administration Policy is available.

Cost to Taxpayers: The Congressional Budget Office (CBO) estimates that implementing H. R. 3202 would cost about $1.5 million in 2015, assuming appropriation of the necessary amounts. That estimate is based on the historical cost of studies and analyses undertaken by those agencies that are similar in scope to those envisioned under the bill. Enacting H. R. 3202 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?: H. R. 3202 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: Congress has the power to enact this legislation pursuant to the following: This bill is enacted pursuant to the power granted to Congress under Article I, Section 8, Clauses 1, 3, and 18 of the United States Constitution.

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.*

H. R. 3846 – The United States Customs and Border Protection Authorization Act
(Rep. Miller, R-MI)

Order of Business: The bill is scheduled to be considered on July 28, 2014, under a motion to suspend the rules and pass the bill, which requires a two-thirds majority for passage.

Summary: H. R. 3846 authorizes border, maritime, and transportation security responsibilities and functions in the Department of Homeland Security and the establishment of the Customs and Border Protection (CBP) agency which has been operating without authorization since 2002. The bill would amend the Homeland Security Act of 2002 by directing Customs and Border Protection in the Department of Homeland Security to establish standard procedures for addressing complaints made against CBP employees and to enhance training for CBP officers and agents.

Section 2 of the legislation would set the requirements of the Commissioner and Deputy Commissioner of the Customs and Border Protection agency to:

- Ensure the interdiction of persons and goods illegally entering or exiting the United States; facilitate and expedite the flow of legitimate travelers and trade;
- Detect, respond to, and interdict terrorists, drug smugglers and traffickers, human smugglers and traffickers, and other persons who may undermine the security of the United States;
- Safeguard the borders of the United States to protect against the entry of dangerous goods; oversee the functions of the Office of International Trade;
- Enforce and administer all immigration laws; develop and implement screening and targeting capabilities, including the screening, reviewing, identifying, and prioritizing of passengers and cargo across all international modes of transportation, both inbound and outbound; enforce and administer the laws relating to agricultural import and entry inspection; and

- Deploy technology to collect the data necessary for the Secretary of Homeland Security to administer the biometric entry and exit data system.

Section 2 also establishes the United States Border Patrol to:

- Serve as the law enforcement office of United States Customs and Border Protection with primary responsibility for interdicting persons attempting to illegally enter or exit the United States or goods being illegally imported to or exported from the United States at a place other than a designated port of entry;

- Deter and prevent illegal entry of terrorists, terrorist weapons, persons, and contraband; and

- Carry out other duties and powers prescribed by the Commissioner.

Section 2 would also authorize the Office of Air and Marine Operations and an Assistant Commissioner to head the division. The bill would also authorize the Office of Field Operations (and would require an annual report on the staffing of the organization), the National Targeting Center, the Office of Intelligence and Investigative Liaison, the Office of International Affairs, and the Office of Internal Affairs. Section 2 mandates that the Commissioner of Customs and Border Protection establish a set of:

- Standard operating procedures for searching, reviewing, retaining, and sharing information contained in communication, electronic, or digital devices encountered by United States Customs and Border Protection personnel at United States ports of entry;

- Standard use of force procedures officers and agents of United States Customs and Border Protection;

- A uniform, standardized, and publically-available procedure for processing and investigating complaints against officers, agents, and employees of United States Customs and Border Protection for violations of professional conduct; and

- An internal, uniform reporting mechanism regarding incidents involving the use of deadly force by an officer or agent of United States Customs and Border Protection.

The preceding procedures established in the section would require the Commissioner to notify the individual subject in the case of a search of information conducted on an electronic device unless the individual is on a Government terrorist watch list. If the individual subject to search of an electronic device is included on a Government-operated or Government-maintained terrorist watch list, the notifications required under the Act do not apply. The Inspector General of the Department of Homeland Security is also directed to develop and annually administer an audit to review whether searches of electronic devices are in compliance. The Commissioner is also directed to require all agents and officers to undergo training and continuing education of Federal legal rulings, and court decisions. Section 2 would also set the standards for short term

detention standards, and access to information on detainee rights at Border Patrol processing centers.

Section 3 of the legislation repeals sections 416, 418, and 443 of the Homeland Security Act of 2002. Section 5 requires the agency to prepare several reports on contract management acquisition and the procurement of personnel, a report on migrant deaths, business transformation initiatives, and a report on unaccompanied alien children apprehended at the border (including the number of unaccompanied aliens, their nationality, age, location of apprehension, the average length of time the alien is in custody, and a description of current activities to discourage efforts to enter in the United States illegally). The section would also require an assessment of port of entry infrastructure. Section 6 directs the Secretary of Homeland Security in coordination with the Secretary of State to engage with the Governments of Canada and Mexico to assess the specific needs of Central American countries to maintain the security of their international borders. The Secretary of Homeland Security is directed to engage with the governments of Caribbean countries as well. Section 7 of H. R. 3846 would express a sense of Congress on the Foreign Language Award Program. Section 8 of the bill mandates that no additional funds are authorized to be appropriated to carry out the Act.

Additional Information: According to the sponsor of H. R. 3846, the Customs and Border Protection agency had been operating without the statutory authorization necessary to support its operations since the agency was transferred to the Department of Homeland Security in 2002. More on the Customs and Border Protection agency can be found here, including a list of fact sheets on U.S. border security.

Committee Action: The bill was introduced on January 10, 2014 and was referred to the House Committee on Homeland Security and the House Committee on Ways and Means. On June 11, 2014, the Committee on Homeland Security marked-up H. R 3846 and ordered it reported (amended) by voice vote. On July 24, 2014, the committee reported (amended) the bill.

Administration Position: No Statement of Administration Policy is available.

Cost to Taxpayers: The Congressional Budget Office (CBO) estimates that implementing H. R. 3846 would cost about $1 million in fiscal year 2015 and less than $500,000 annually thereafter, from appropriated funds, mostly for the required reports. According to Customs and Border Protection (CBP), much of the information needed for those reports has already been compiled. Enacting the legislation 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?: H. R. 3846 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: 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.*

H. R. 3696 – The National Cybersecurity and Critical Infrastructure Protection Act (Rep. McCaul, R-TX)

Order of Business: The bill is scheduled to be considered on July 28, 2014, under a motion to suspend the rules and pass the bill, which requires a two-thirds majority for passage.

Summary: H. R. 3696 amends the Homeland Security Act of 2002 by requiring the Secretary of Homeland Security to conduct cybersecurity activities. The bill also codifies the Department of Homeland Security's role in responding to cyber attacks and breaches involving the Information Technology (IT) systems of federal civilian agencies and critical infrastructure in the United States.

Title I of the bill amends the Homeland Security Act of 2002 by directing the Secretary of Homeland Security in collaboration with the heads of other appropriate Federal Government entities, to conduct activities for cybersecurity purposes to provide shared situational awareness and enable real-time, integrated, and operational actions to protect from, prevent, mitigate, respond to, and recover from cyber incidents.

Title I directs the Secretary of Homeland Security to coordinate with Federal, State, and local governments, national laboratories, critical infrastructure owners, critical infrastructure operators, and other cross sector coordinating entities to:

- Facilitate a national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure from cyber threats;
- Ensure that Department of Homeland Security policies and procedures enable critical infrastructure owners and critical infrastructure operators to receive real-time, actionable, and relevant cyber threat information;
- Seek industry sector-specific expertise on security strategies and the cost effectiveness of the allocation of Federal resources;
- Provide education and assistance to such owners and operators on how they may use protective measures and countermeasures to strengthen the security and resilience of critical infrastructure; and

- Coordinate a research and development strategy to facilitate and promote advancements and innovation in cybersecurity technologies.

The Secretary is also directed to manage Federal efforts to secure and protect the resiliency of Federal civilian information systems. The Secretary is also mandated to designate critical infrastructure sectors including chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation systems, and water and wastewater systems. In doing so, H. R. 3696 requires the Secretary to designate critical infrastructure sectors; and to recognize, for each sector, a Sector Coordinating Council (SCC) and at least one Information Sharing and Analysis Center (ISAC). Each critical infrastructure sector is designated to a corresponding Federal agency. This section reallocates funds, a minimum of $25,000,000 per year for three years, from the Cybersecurity and Communications Office for operations support at the National Cybersecurity and Communications Integration Center for all recognized ISACs.

Section 104 of the bill establishes the National Cybersecurity and Communications Integration Center, as a federal civilian information sharing interface to:

- Provide shared situational awareness to enable real-time, integrated, and operational actions across the federal government; and

- Share cyber threat information among Federal, state, and local government entities, ISACs, private entities, and critical infrastructure owners and operators that have information sharing relationships.

The Secretary of Homeland Security is directed to submit a report to Congress that summarizes major cyber incidents involving Federal civilian agency information systems and provides aggregate statistics on the number of breaches, the extent of any personally identifiable information that was involved, the volume of data exfiltrated, the consequential impact, and the estimated cost of remedying such breaches. The Secretary is also directed to submit a report on the capability and capacity of the National Cybersecurity and Communications Integration Center to carry out its mission. The Comptroller General is also mandated to submit a report on the effectiveness of the Center as well.

Section 105 of the bill would establish Cyber Incident Response Teams to provide technical assistance and recommendations to federal, state, and local government entities, private entities, and critical infrastructure owners and operators.

The Secretary, in coordination with the Sector Coordinating Councils, Information Sharing and Analysis Centers, and Federal, State, and local governments develop, regularly update, maintain, and exercise a National Cybersecurity Incident Response Plan.

Section 106 directs the Secretary of Homeland Security to submit to Congress a report on the feasibility of making the Cybersecurity and Communications Office of the Department an operational component of the Department. The section would also redesignate the National

Protection and Programs Directorate as the Cybersecurity and Infrastructure Protection Directorate.

Title II of the bill would direct the Director of the National Institute of Standards and Technology, in coordination with the Secretary of Homeland Security to facilitate and support the development of a voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks to critical infrastructure. The section stipulates that information shared with or provided to the Director of the National Institute of Standards and Technology or the Secretary of Homeland Security may not be used by any Federal, State, or local government department or agency to regulate the activity of any private entity.

Section 201 requires the Secretary of Homeland Security to meet biannually with each Sector Coordinating Council and to submit annual reports to Congress on the state of cybersecurity in each sector. Section 202 amends the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 by expanding liability protections for technology providers to include designated cybersecurity technologies deployed in defense of qualifying cyber incidents. A qualifying cyber incident that meets the requirements of this section would include:

- Unlawful or unauthorized access incidents;
- Disruption of the integrity, operation, confidentiality, or availability of programmable electronic devices or communication networks;
- Misappropriation, corruption, or disruption of data, assets, information, or intellectual property; and
- Harm inside or outside the United States that results in damages, disruptions, or casualties severely affecting the U.S. population, infrastructure, economy, national morale, or federal, state, local, or tribal government functions.

Section 203 would prohibit this Act from being construed to create or authorize any new regulations or additional federal government regulatory authority, or authorize the appropriation of any additional funds.

Section 204 would mandate that no additional funds are authorized to be appropriated to carry out the Act and the amendments made by the Act.

Section 205 mandates that nothing in the Act shall permit the Department of Homeland Security to engage in the monitoring, surveillance, exfiltration, or other collection activities for the purpose of tracking an individual's personally identifiable information.

Section 206 directs the Secretary of Homeland Security to determine the feasibility and potential benefit of developing a visiting security researchers program from academia, including cybersecurity scholars at the Department of Homeland Security's Centers of Excellence.

Section 207 directs the Secretary of Homeland Security, in coordination with the heads of other departments and agencies, as necessary, to enter into an agreement with the National Research Council to conduct research of the future resilience and reliability of the Nation's electric power transmission and distribution system.

Title III of the bill directs the Secretary to develop and issue comprehensive occupation categories for individuals performing activities in furtherance of the cybersecurity mission of the Department of Homeland Security. This section of the bill reflects the Homeland Security Cybersecurity Boots-on-the-Ground Act, identical to H. R. 3107. The Secretary is directed to assess the readiness and capacity of the workforce of the Department to meet its cybersecurity mission. The bill directs the Secretary of Homeland Security develop, maintain, and, as necessary, update, a comprehensive workforce strategy that enhances the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department. The Secretary is also required to submit to the Government Accountability Office (GAO) information on the cybersecurity workforce assessment. The Secretary is directed to:

- Submit a report on the feasibility of establishing a Cybersecurity Fellowship Program to offer a tuition payment plan for undergraduate and doctoral candidates who agree to work for the Department for an agreed-upon period of time.

- Authorize and establish as positions in the excepted service, appoint individuals to such positions, fix pay, and pay a retention bonus to any employee appointed if the Secretary determines that such is needed to retain essential personnel.

Additional Information: The report (H. Rept. 113-550) accompanying H. R. 3696 can be found here. A list of organizations and companies, (including the Boeing Company, the National Defense Industrial Association, AT&T, Verizon, Entergy, and the American Chemistry Council), in support H. R. 3696 can be found here. On op-ed by the Chairman of the House Committee on Homeland Security on H. R. 3696 can be found here.

Committee Action: The bill was introduced on December 11, 2013, and was referred to the House Committee on Homeland Security, the House Committee on Science, Space, and Technology, and the House Committee on Oversight and Government Reform. On February 5, 2014, the bill was ordered to be reported (amended) by voice vote by the House Committee on Homeland Security. On July 23, 2014, H. R. 3696 was reported by the Committee on Homeland Secuirty (amended) by voice vote.

Administration Position: No Statement of Administration Policy is available.

Cost to Taxpayers: The Department of Homeland Security currently conducts many of the activities covered by H. R. 3696 and has received approximately $800 million so far in fiscal year 2014 for its cybersecurity activities. Some provisions in the bill would expand existing programs, provide additional authorities, or add new requirements beyond the agency's current efforts. Assuming the appropriation of the necessary amounts, the Congressional Budget Office (CBO) estimates that implementing the bill would cost an additional $160 million over the 2015-

2019 period. Pay-as-you-go procedures do not apply to this legislation because it would not affect direct spending or revenues. 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?: H.R. 3696 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA).

Constitutional Authority: Congress has the power to enact this legislation pursuant to the following: the Constitutional authority on which this bill rests is the power of Congress to make all laws necessary and proper for executing powers vested by the Constitution, as enumerated in Article I, Section 8, Clause 18 of the United States Constitution.

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.*

H. R. 2952 – The Critical Infrastructure Research and Development Act (Rep. Meehan, R-PA)

Order of Business: The bill is scheduled to be considered on July 28, 2014, under a motion to suspend the rules and pass the bill, which requires a two-thirds majority for passage.

Summary: H. R. 2952 amends Title III of the Homeland Security Act of 2002 by directing the Secretary of Homeland Security, acting through the Under Secretary of Homeland Security for Science and Technology, to transmit to Congress within 180 days of the bill's enactment, a strategic plan to guide the overall direction of Federal physical security and cybersecurity technology research and development efforts for protecting critical infrastructure, including against all threats. The Secretary is also directed to submit once every two years after the initial strategic plan, an update of the plan that would include:

- An identification of critical infrastructure security risks and any associated security technology gaps;
- A set of critical infrastructure security technology needs;
- An identification of laboratories, facilities, modeling, and simulation capabilities that will be required to support the research, development, demonstration, testing, evaluation, and acquisition of the security technologies;
- An identification of current and planned programmatic initiatives for fostering the rapid advancement and deployment of security technologies for critical infrastructure protection; and

- A description of progress made with respect to each critical infrastructure security risk, associated security technology gap, and critical infrastructure technology need identified in the preceding strategic plan.

H. R. 2952 directs the Secretary of Homeland Security through the Under Secretary of Homeland Security for Science and Technology to report to Congress the Department's utilization of public-private research and development consortiums for accelerating technology development for critical infrastructure protection. The report would include:

- A summary of the progress and accomplishments of on-going consortiums for critical infrastructure security technologies;

- A prioritized list of technology development focus areas that would most benefit from a public-private research and development consortium; and

- A proposal for implementing an expanded research and development consortium program, including an assessment of feasibility and an estimate of cost, schedule, and milestones.

The bill would also direct the Secretary of Homeland Security through the Under Secretary of Homeland Security for Science and Technology, and in coordination with the Under Secretary for the National Protection and Programs Directorate, to designate a technology clearinghouse for rapidly sharing proven technology solutions for protecting critical infrastructure. The legislation would also require the Department of Homeland Security's Privacy Officer to annually review the clearinghouse process to evaluate its consistency with fair information practice principles. No later than 2 years after the enactment of the Act, the Comptroller General of the United States is directed to conduct an independent evaluation, and submit to Congress a report on such clearinghouses. Section 4 of the bill mandates that no additional funds are authorized to be appropriated to carry out the Act.

Additional Information: 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.

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 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. 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.*

H. R. 3107 – The Homeland Security Cybersecurity Boots-on-the-Ground Act (*Rep. Clarke*, D-NY)

Order of Business: The bill is scheduled to be considered on July 28, 2014, under a motion to suspend the rules and pass the bill, which requires a two-thirds majority for passage.

Summary: H. R. 3107 would require the Secretary of Homeland Security to establish cybersecurity occupation classifications, assess the cybersecurity workforce, and develop a strategy to address identified gaps in the cybersecurity workforce. Not later than 180 days after the date of the enactment of this section and annually thereafter, the Secretary of Homeland Security is directed to assess the readiness and capacity of the workforce of the Department to meet its cybersecurity mission including:

- Information on where cybersecurity positions are located within the Department, specified in accordance with the cybersecurity occupation categories;
- Information on which cybersecurity positions are performed by permanent full time departmental employees, individuals employed by independent contractors, individuals employed by other Federal agencies, including the National Security Agency;
- The number of individuals hired by the Department pursuant to the authority granted to the Secretary in 2009 to permit the Secretary to fill 1,000 cybersecurity positions across the Department over a three year period;
- Information on vacancies within the Department's cybersecurity supervisory work force;

- Information on the percentage of individuals within each cybersecurity occupation category who received essential training to perform their jobs; and

- Information on recruiting costs incurred with respect to efforts to fill cybersecurity positions across the Department of Homeland Security.

Additionally, the bill directs the Secretary of Homeland Security to develop, maintain, and, as necessary, update, a comprehensive workforce strategy that enhances the readiness, capacity, training, recruitment, and retention of the cybersecurity workforce of the Department. The Secretary of Homeland Security is also directed to establish and maintain a process to verify that individuals employed by independent contractors who serve in cybersecurity positions at the Department receive initial and recurrent information security training comprised of general security awareness training necessary to perform their job functions, and role-based security training that is commensurate with assigned responsibilities. In doing so, the Secretary is directed to submit to Congress annual updates regarding the cybersecurity workforce assessment.

The Secretary is also required to submit to the Government Accountability Office (GAO) information on the cybersecurity workforce assessment. GAO is then mandated to submit to Congress a study on such assessment and workforce strategies. The Secretary shall also submit a report on the feasibility of establishing a Cybersecurity Fellowship Program to offer a tuition payment plan for undergraduate and doctoral candidates who agree to work for the Department for an agreed-upon period of time. The Secretary is also authorized to establish positions in the excepted service, appoint individuals to such positions, fix pay, and pay a retention bonus to any employee appointed if the Secretary determines that such is needed to retain essential personnel. Before announcing the payment of a bonus, the Secretary is required to notify Congress and to submit a report that discusses the processes used by the Secretary in accepting applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by a qualified employee.

Section 3 of the bill stipulates that no additional amounts are authorized to be appropriated by reason of the Act or the amendments made by the Act.

Additional Information: The report (H. Rept. 113-294) accompanying H. R. 3107 can be found here.

Committee Action: The bill was introduced on September 17, 2013 and was referred to the House Committee on Homeland Security. On October 29, 2013, the bill was marked-up and ordered to be reported (amended) by voice vote. On December 12, 2013, the bill was reported (amended) by the House Committee on Homeland Security.

Administration Position: No Statement of Administration Policy is available.

Cost to Taxpayers: The bill also would require the Department of Homeland Security (DHS) to maintain documentation verifying that contractors who serve in cybersecurity roles at DHS receive the training necessary to perform their assigned responsibilities. The Congressional

Budget Office (CBO) anticipates that effort would require additional staffing and resources. Based on the cost of similar personnel, CBO estimates that implementing that requirement would cost approximately $2 million over the 2014-2019 period, subject to the availability of appropriated funds. Enacting H.R. 3107 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?: H. R. 3107 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: this bill, The Homeland Security Cybersecurity Boots-on- the-Ground Act, is enacted pursuant to the power granted to Congress under Article I of the United States Constitution and its subsequent amendments, and further clarified and interpreted by the Supreme Court 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.*

Democrat Motion to Instruct Conferees on H.R. 3230 — (Rahall –D, WV)

Order of Business: Representative Rahall announced his intention to offer a motion to instruct conferees on H.R. 3230 on July 25, 2014.

Summary: Representative Rahall's motion would instruct the House managers on the conference committee to end their disagreement with section 203 of the Senate amendment to H.R 3230 as well as support the Senate amendment in its totality. A vote in favor of this motion would indicate support for section 203 of the Senate Amendment to the House bill which allows for the use of unobligated funds to hire additional health care providers for the Veterans Health Administration. For fiscal years 2014 and 2015, unobligated funds in the Medical Services account, Medical Support and Compliance account, and the Medical Facilities account will be made available to the Veterans Health Administration for hiring addition health care provides. These funds will remain available until expended.

In addition, the Rahall motion instructs the conferees to recede from the House amendment and agree with the Senate amendment in all other instances. The House has previously voted on four motions to instruct conferees to concur in the Senate Amendment. The motion offered by Representative Sinema (D-AZ) failed by a vote of 198-220; the motion offered by Representative Barber (D-AZ) which contained instructions to recede from the House amendment failed by a vote of 191-207; the motion offered by Representative Peters which

contained instructions to recede from the House amendment, failed by a vote of 205-207; and the motion offered by Representative Brownley (D-CA) contained instructions to recede from the House amendment, failed by a vote of 213-193.

CBO estimates the Senate amendment to H.R. 3230 would result in additional direct spending totaling $35 billion over fiscal years 2014-2024.

Additional Background: The House may vote to instruct its conferees under three different circumstances. First, before the conferees are appointed; second, 20 calendar days and 10 legislative days after the conferees were appointed (if they had not yet filed a conference report); finally, when a conference report is recommitted to conference. The motion to instruct only instructs House conferees and not those that have been appointed by the Senate. It is important to note the instructions to conferees are not binding; therefore, a point of order cannot be sustained against the conference report in the event it is inconsistent with the instructions voted out of the House.

Committee Action: Motions to instruct are not referred to committee.

Cost to Taxpayers: The motion itself would yield no new costs to taxpayers. For costs associated with the underlying policy of the motion, please refer to the CBO score linked in the summary above.

Constitutional Authority: According to House rules, a constitutional authority statement is not needed for motions to instruct.

RSC Staff Contact: Rebekah Armstrong, Rebekah.Armstrong@mail.house.gov, 202-226-0678

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.*