RSC Republican Study Committee
Rep. Jeb Hensarling (R-TX), Chairman
Russ Vought, Executive Director
132 Cannon House Office Building
Washington, DC 20515
www.house.gov/hensarling/rsc
Ph (202) 226-9717 / fax (202) 226-1633

Legislative Bulletin……..……June 20, 2008

Contents:

Summary of the Bill Under Consideration Today:

Total Number of New Government Programs: Numerous

Total Cost of Discretionary Authorizations: Such sums as appropriated

Effect on Revenue: $0

Total Change in Mandatory Spending: 0

Total New State & Local Government Mandates: 0

Total New Private Sector Mandates: 1

Number of *Bills* Without Committee Reports: 1

Number of *Reported* Bills that Don't Cite Specific Clauses of Constitutional Authority: 0

H.R. 6304—FISA Amendments Act of 2008
(*Reyes, D-TX*)

Summary: H.R. 6304 would overhaul and reauthorize the Foreign Intelligence Surveillance Act of 1978. Most notably, the compromise legislation would provide an avenue for telecommunications companies to protect themselves against lawsuits stemming from intelligence gathering assistance rendered to the federal government.

The bill would also allow the U.S. intelligence community, in emergency circumstances, to conduct surveillance on foreign targets that may be communicating with persons inside the U.S. without prior FISA court approval, though every acquisition obtained prior to court approval would be subject to review within seven days. The bill would require relevant federal agencies

to review the Administration's warrantless surveillance program and report to Congress within one year. In addition, H.R. 6304 would require the intelligence community to provide Congress with periodic reports regarding surveillance programs and would place more Congressional oversight on the FISA court. The legislation would sunset on December 31, 2012.

Below is a summary of the bill's major compromises, followed by background on FISA and a summary of the bill's main provisions.

Protection for Telecommunication Providers: H.R. 6304 would set up a process for Federal district courts to review both prospective and retroactive claims relating to telecommunications companies' assistance in obtaining intelligence surveillance acquisitions for the government following September 11, 2001. With respect to retroactive liability protection, all pending cases would be sent to U.S. district courts. The bill would require the Attorney General to certify to a district court that one of two situations occurred. Either the assistance provided by the carrier was authorized by the President, designed to detect or prevent a terrorist attack against the U.S. after September 11, and could be verified by a written request or a series of requests to the carrier, or the telecommunications company in question did not provide assistance to the intelligence community. The written request for assistance must have informed the communications provider that the activity requested was authorized by the President, and was lawful.

Under H.R. 6304, if a district court determines that a telecommunications company assisted the intelligence community in response to a written request from the President, or determines that no assistance was provided, any pending lawsuit would be dismissed.

Authorizing Electronic Surveillance in Foreign Countries: H.R. 6304 would allow the Director of National Intelligence (DNI) and the Attorney General (AG) to authorize the acquisition of electronic intelligence from persons in foreign countries, with the approval of the FISA court (FISC). However, the bill authorizes the AG and the DNI to initiate an acquisition without approval from the FISC if the AG and the DNI determine that "exigent circumstances" exist due to the fact that intelligence important to the national security of the U.S. could be lost or not timely acquired while waiting for a FISC review. If the AG and the DNI make such a determination, they would be required to submit a retroactive certification to the FISC within seven days.

Acquisitions Targeting U.S. Persons Outside the U.S.: The bill would prohibit any element of the intelligence community from intentionally targeting a U.S. person reasonably believed to be located outside the U.S. under circumstances in which the target has a "reasonable expectation of privacy" and a warrant would be required in the U.S., unless the FISC has approved an order to target such person or the AG has authorized an emergency acquisition.

Oversight and Review of Previous Actions: H.R. 6304 would require the Inspectors General of the Department of Justice and assorted Intelligence Community agencies to conduct a review of all previous activities of the Terrorist Surveillance Program within their jurisdictions and report to Congress within one year.

Background: Historically, the U.S. government has not been required to obtain a court order to acquire electronic surveillance information from foreign persons operating overseas. However, revelations of possible abuses of electronic surveillance for national security purposes were reported in the 1970s and Congress responded by passing legislation to provide a statutory structure for gathering electronic surveillance intelligence. The Foreign Intelligence Surveillance Act of 1978 (FISA) was initially established to provide a process for obtaining a court order to conduct foreign intelligence surveillance within the U.S. The law now provides a structure for gathering intelligence through electronic surveillance, physical searches, trap and trace devices (similar to caller ID), and business records. Due to rapid changes in telecommunications technology, FISA frequently required government officials to obtain a court order to gather information on suspected terrorists and various other foreign intelligence targets located overseas, but possibly communicating with persons inside the U.S. In order to address concerns that FISA was restricting the intelligence community from obtain vital intelligence information abroad, the House of Representatives passed S. 1927, the Protect America Act (PAA) on August 4, 2007, by a vote of 227—183.

The PAA extended provisions of FISA to allow the U.S. intelligence community to conduct surveillance on non-U.S. persons located overseas without obtaining permission from the FISA Courts. In addition, the PAA made the FISA Courts responsible for reviewing surveillance information to ensure that collection was targeted at non-U.S. persons located abroad. The bill also protected telecommunications companies that assisted intelligence officials gather information following September 11, 2001, from private lawsuits. The provisions of the PAA (with the exception of Section I) were scheduled to sunset on February 1, 2008, giving Congress 180 days to produce an acceptable long-term extension of the bill.

By late January 2008, the Congress had failed to act on legislation to permanently extend key FISA provisions. Democratic House leadership filed a thirty day extension to the PAA, which would have extended the provisions through March 2008. The Bush Administration quickly came out in opposition to the lengthy extension and urged Congress to act on S. 2248, a bi-partisan compromise that the Administration was prepared to sign. In a strongly worded Statement of Administration Policy (SAP), the Administration stated that it would not approve short-term extensions of the PAA and demanded action from Congress. The SAP stated that "Congress has had almost six months to pass new legislation that will ensure that our Intelligence Community retains the tools it needs to protect the country. [The thirty day extension], however, is deficient and unacceptable." The President eventually compromised with Congress signed a fifteen day extension which authorized the provisions of PAA through February 15, 2008.

On Tuesday, February 12, 2008, the Senate passed a long-term FISA extension, the FISA Amendments Act of 2007 (S. 2248), by a vote of 68-29. The bi-partisan bill was introduced by Sen. Rockefeller (D-WV) and was considered acceptable to the Bush Administration and the Director of National Intelligence (DNI), Mike McConnell. The legislation would have allowed the U.S. intelligence community to conduct surveillance on non-U.S. persons located abroad and granted retroactive immunity to telecommunications companies that assisted the U.S. in obtaining information.

Despite calls for immediate consideration of S. 2248, House majority leadership opted to consider H.R. 5349—a short-term extension—in lieu of a long-term, bi-partisan solution. Under a veto threat from the Administration, and in the face of Democrat opposition, H.R. 5349 was defeated on February 15, and the PAA expired the following day.

In the intervening months, House and Senate Leaders from both parties have negotiated with the Director McConnell and Attorney General Michael Mukasey to develop a compromise bill that would be acceptable to the intelligence community. H.R. 6304 is the result of those negotiations. The legislation would allow the U.S. intelligence community to conduct surveillance on suspects in foreign nations without FISC authority in emergency situations and provide a means by which telecommunications companies could obtain legal immunity. In a letter to House Speaker Nancy Pelosi dated June 19, Director McConnell and Attorney General Mukasey both stated that they would recommend the President sign H.R. 6304 if it were presented to him.

Summary of the Major Provisions of H.R. 6304: What follows is a summary of some of the major provisions of H.R. 6304. The summary includes only highlights of H.R. 6304.

Additional Procedures for Authorizing Certain Electronic Surveillance

- Authorizes Director of National Intelligence (DNI) and the Attorney General (AG) to jointly authorize the acquisition of foreign intelligence information for up to one year on persons reasonably believed to be outside the U.S. An acquisition authorized under this section may not:
  - -- Intentionally target persons known to be located in the U.S.
  - -- Intentionally target a person reasonably believed to be outside the U.S. for the purpose of acquiring intelligence on a person known to be in the U.S.
  - -- Be conducted in a manner that is inconsistent with the fourth amendment
  - -- Intentionally target a United States person reasonably believed to be located outside the United States, except in accordance with other sections in the bill.

- Requires the AG, in coordination with the DNI, to develop and adopt targeting, minimization, and certification procedures to regulate surveillance acquisitions and ensure that targets are outside the U.S. The standards would be subject to the review of the FISC.

- Stipulates that the DNI and the AG must provide the Foreign Intelligence Surveillance Court (FISC) with a written certification ensuring that all acquisitions are limited to persons reasonably believed to be outside the U.S. A certification submitted by the AG and the DNI must be approved by the FISC before the acquisition is undertaken.

- Authorizes the AG and the DNI to authorize an acquisition without approval from the FISC if the AG and the DNI determine that "exigent circumstances" exist due to the fact that intelligence important to the national security of the U.S. could be lost or not timely acquired while waiting for a FISC review. If the AG and the DNI make such a

determination, they would be required to submit a certification to the FISC within seven days.

- Allows the AG and the DNI to direct an electronic communication service provider to supply the government information and assistance needed to accomplish an intelligence acquisition in a manner that will protect the secrecy of the acquisition. The bill would allow the service provider to maintain certain records of the acquisition and require the government to provide the services provider with compensation.

- Allows a communications provider to appeal to the FISC in an effort to challenge a government request for assistance.

- Authorizes the FISA Court the power to compel a communications company to comply with a request for assistance if the companies challenge to the request was denied by FISC.

Certain Acquisitions Inside the U.S. of U.S. Persons Outside the U.S.

- Authorizes electronic surveillance targeting of U.S. person reasonably believed to be located outside the U.S. if it is approved by the FISA Court. Targeting under this provision would cease if, at any time during the surveillance, it is reasonably believed that the target is within the U.S.

- Requires the AG to submit an application to the FISA Court to obtain such a surveillance order. The application would have to include, among other things:
  -- The identity of the federal officer making the application
  -- The identity, if known, of the U.S. person being targeted.
  -- A statement to justify the applicant's belief that the target is reasonably believed to be outside the U.S. and is a foreign power or an agent of a foreign power
  -- A description of the nature of the information sought
  -- An official certification made by the AG

- Limits the duration of an order under this section to 90 days after the FISA Court approves the order.

- Authorizes the AG to issue an emergency order under this section if he or she reasonably determines an emergency situation exists. The AG is required to notify a FISA Court judge of the emergency acquisition. An emergency acquisition authorized under this section would expire in seven days if a FISA Court order was not authorized.

- Prohibits any of the evidence retrieved in the course of an emergency acquisition from being used if the AG's application is eventually denied by the FISA Court or if the AG fails to file an application for approval before the 7 day period expires.

- Releases any electronic communication service provider from liability in connection with assistance provided to the government in an acquisition targeting a U.S. person reasonably believed to be located outside the U.S.

- Authorizes the government to file an appeal to the FISC if an application was denied following an emergency acquisition.

Other Acquisitions Targeting U.S. Persons Outside the U.S.

- Prohibits any element of the intelligence community from intentionally targeting a U.S. person reasonably believed to be located outside the U.S. under circumstances in which the target has a "reasonable expectation of privacy" and a warrant would be required in the U.S., unless the FISC has approved an order to target such person or the AG has authorized an emergency acquisition.

- Requires the AG to submit an application to the FISA Court to obtain such a surveillance order. The application would have to include, among other things:
  -- The identity, if known, of the U.S. person being targeted.
  -- A statement to justify the applicant's belief that the target is reasonably believed to be outside the U.S. and is a foreign power or an agent of a foreign power
  -- Proposed minimization standards
  -- A description of the nature of the information sought
  -- An official certification made by the AG

- Authorizes the AG to issue an emergency order under this section if he or she reasonably determines an emergency situation exists. The AG is required to notify a FISA Court judge of the emergency acquisition. An emergency acquisition authorized under this section would expire in seven days if a FISA Court order was not authorized.

Joint Applications and Concurrent Authorization

- Allows a FISA Court judge to approve a joint application for acquisition of information from a U.S. if the proposed acquisition will be conducted both inside and outside the U.S.

- Allows the AG, without an approved FISA Court order, to acquire foreign intelligence information from a U.S. person reasonably believed to be overseas if the FISA Court has already authorized electronic surveillance or physical searches on the individual.

Congressional Oversight

- Requires the AG to submit a report to the appropriate committees in Congress detailing any certifications, directives, or orders made by the FISA Court, DNI, or the AG and a description of the judicial review process during the reporting session.

Statement of Exclusive Means

- States that FISA (as amended by this Act) is the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.

Submittal of Court Orders to Congress

- Requires the AG to submit, within 45 days of enactment, a copy of any decision, order, or opinion issued by the FISC that includes significant construction or interpretation of the Foreign Intelligence Surveillance Act over the past five years.

Issuance of an Order

- Increases the amount of time the AG has to obtain a FISC order after authorizing an emergency authorization for acquisition from 3 days to 7 days.

Emergency Pen Registers and Trap Trace Devices

- Increases the amount of time the AG has to obtain a FISC order after authorizing the installation of emergency installation pen register or trap and trace devices from 2 days to 7 days.

Committee Action: H.R. 6304 was introduced on Thursday, June 19, 2008, and referred to the Committee on the Judiciary and the Select Committee on Intelligence, which took no official action.

Cost to Taxpayers: A CBO score for H.R. 6304 was not available at press time.

Does the Bill Expand the Size and Scope of the Federal Government? Yes, the bill alters current regulations and requirements regarding electronic surveillance and foreign intelligence information gathering.

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates? A CBO score for H.R. 6304 was not available at press time.

Does the Bill Comply with House Rules Regarding Earmarks/Limited Tax Benefits/Limited Tariff Benefits? A Committee Report citing compliance with House Rules Regarding Earmarks/Limited Tax Benefits/Limited Tariff Benefits was not available at press time.

Constitutional Authority: A Committee Report citing constitutional authority was not available at press time.

RSC Staff Contact: Andy Koenig; andy.koenig@mail.house.gov; 202-226-9717.