



**Side-by-Side Analysis  
Restoration of Freedom of Information Act of 2003  
and the Homeland Security Act of 2002**

The following is a side-by-side analysis of key issues in the Critical Infrastructure Information subtitle of the Homeland Security Act of 2002. The Critical Infrastructure Information provisions address a new Freedom of Information Act exemption for information on infrastructure vulnerabilities voluntarily submitted to the Department of Homeland Security and additional protections that information may receive. The analysis compares the subtitle passed last year and a bill being offered by Sens. Patrick Leahy (D-VT), Carl Levin (D-MI), Joseph Lieberman (D-CT), James Jeffords (I-VT), and Robert Byrd (D-WV) to replace the current subtitle. The new bill utilizes bipartisan language developed last year during negotiations with Sen. Robert Bennett (R-UT). This compromise subtitle uses the language the Senate Governmental Affairs Committee originally passed for the Homeland Security Act of 2002.

Issue	“Restore FOIA” Bill	Homeland Security Act
<b>Scope of FOIA Exemption</b>	Creates a FOIA exemption limited to "records" submitted by the private sector, not "information" from the private sector. Records, the standard category used in FOIA exemptions, refer to physical and well-defined communications (documents, reports, emails, etc.).	Uses the new and more expansive term "information" for the FOIA exemption, which could include telephone calls, conversations, verbal answers (if the information is not required). This new and untested category could create confusion and hamper government's ability to manage information efficiently.
<b>Definition of Critical Infrastructure Information</b>	Limits the exemption to records pertaining to "the vulnerability of and threats to critical infrastructure (such as attacks, response and recovery efforts)"	Applies the exemption to the broader and more vague category of any "critical infrastructure information" which could allow information not directly related to vulnerabilities to inappropriately receive the subtitle's protections.
<b>Definition of Voluntarily Submitted</b>	Defines voluntarily more narrowly as submissions in the <b>absence</b> of legal authority. This requires the information to fall outside of the bounds of current regulatory authority and that the government could not obtain the records except by voluntary submission.	Defines voluntarily broadly as submissions in the absence of the <b>exercise</b> of legal authority. This implies that legal authority to require the documents may exist but is not currently being exercised yet the companies may be credited as voluntarily submitting the information. Information and details that agencies don't currently ask for could be submitted and protected under this subtitle before regulators have the opportunity to exercise their authority.
<b>Agency Oversight</b>	Allows and anticipates agency review establishing clearly that portions of records that are not covered by the exemption should be released pursuant to FOIA requests.	Does not allow for any agency review and fails to provide any direction for handling records that only partially contain critical infrastructure information.

Promoting Government Accountability

1742 Connecticut Ave NW  
Washington, DC 20009

tel: 202.234.8494  
fax: 202.234.8584

email: [ombwatch@ombwatch.org](mailto:ombwatch@ombwatch.org)  
web: <http://www.ombwatch.org>

<b>Government Use of Information</b>	Sets no limits or restrictions on the government's use and sharing of the records within the government. The only restriction upon government agencies is to not disclose the record to the public.	Significantly limits the government's ability to act upon the information received by prohibiting any use or disclosure, even to other federal agencies, of the information except for purposes stated in the Act.
<b>State &amp; Local Disclosure laws</b>	Does not preempt any state or local disclosure laws for information obtained from anyplace other than the Department of Homeland Security. Does not restrict the use of the information by state agencies.	Preempts all state and local disclosure and information access laws. State agencies are restricted in their use of the information in the same manner as federal agencies.
<b>Criminal Penalties</b>	Does not criminalize disclosure of critical infrastructure information or preempt any whistleblower protections.	Preempts whistleblower protections for government employees and attaches criminal penalties including a fine and up to one year in jail for disclosure of critical infrastructure information.
<b>Immunity</b>	Does not provide any civil immunity to companies submitting information.	Information cannot be used in civil suits by government or private parties. Information would be more difficult to use in civil suits where the information was obtained independently. Provisions could potentially impede criminal investigations & prosecutions.
<b>Agencies covered</b>	Clarifies that records submitted to other agencies are not covered, even if the same document is also submitted to the DHS.	Wording allows for the provision to be interpreted more broadly and potentially allows the exemption to apply to information submitted to other agencies that is also submitted voluntarily to Dept. of Homeland Security.
<b>FACA</b>	Does not exempt any communications of information from the requirements of the Federal Advisory Committee Act.	Exempts all communication of critical infrastructure information from the open meetings and other requirements of the Federal Advisory Committee Act.
<b>Congressional Oversight</b>	Does not restrict Congressional use or disclosure of the information. Requires a report on the provisions' implementation be made to Congress within 18 months of enactment.	May limit the ability of members of Congress to disclose or use critical infrastructure information. Does not require that a report on the implementation of these provisions be made to Congress.