Sensitive But Unclassified Provisions In the Homeland Security Act of 2002

Latest Revision June 11, 2003

Apparently a seemingly innocuous subtitle in the Homeland Security Act of 2002 slipped under the radar during the legislative debates, with provisions that could prove more damaging to access to government information than the Critical Infrastructure Information subtitle. The provisions address the management, protection and sharing of homeland security information, both classified and "sensitive but unclassified." The policies that address the Sensitive But Unclassified information hold the potential to envelope tremendous quantities of information in a shroud of secrecy called homeland security.

The provisions are under Title VIII, Subtitle I, which deals with "Information Sharing." This subtitle establishes procedures for sharing "homeland security" information among federal, state and local authorities. In addressing this, the law also requires the President to "prescribe and implement procedures" for safeguarding "sensitive but unclassified" information, not just for states and localities. The law also allows the President to set limits on the use and reuse of such information given to states and localities. The law is unclear what vehicle the President is to use to develop these procedures (e.g., a notice and comment rulemaking). There is no requirement for public comment.

Protecting Sensitive But Unclassified

The Subtitle provides findings that link the treatment of classified information and Sensitive But Unclassified information, and includes references to protecting information. Additionally, in one provision the legislation even infers that the information, including sensitive but unclassified, is already protected.

> Sec. 891(b)(3) The Federal Government collects, creates, manages, and protects classified and sensitive but unclassified information to enhance homeland security.
>
> Sec. 891(b)(5) The needs of State and local personnel to have access to relevant homeland security information to combat terrorism must be reconciled with the need to preserve the protected status of such information and to protect the sources and methods used to acquire such information.

Following the findings, the law spells out very specific requirements for both "identifying" and "safeguarding" sensitive but unclassified homeland security information.

> Sec. 892(a)(1)(B) identify and safeguard homeland security information that is sensitive but unclassified;

This simple statement is very vague and could be interpreted very broadly. This provision could be used to justify sealing away almost any kind of information with no or little review. "Identifying" information could potentially include governmental and non-governmental

information that meets the definition of Sensitive But Unclassified information. For instance, the procedures could "identify" certain scientific topics as sensitive but unclassified homeland security information, and restrict publication of research. Safeguarding information is also vague enough that the term could potentially withhold excessive amounts of information that is currently in public domain. The procedures to "safeguard" the information could even affect the manner in which agencies implement the Freedom of Information Act (FOIA). The practically unchecked restrictions on information that may result from these provisions would certainly reduce media's access to government and in the process diminish the government's accountability to the public.

Definitions

At no point does the Subtitle define "identify," "safeguard" or "sensitive but unclassified," leaving the requirements wide open to any number of interpretations. "Homeland security information" is defined, but has several clauses that are open enough to allow vast quantities of information to qualify.

> (1) The term ''homeland security information'' means any information possessed by a Federal, State, or local agency that—
>
> (A) relates to the threat of terrorist activity;
>
> (B) relates to the ability to prevent, interdict, or disrupt terrorist activity;
>
> (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or
>
> (D) would improve the response to a terrorist act.

Several of these definitions could be interpreted very broadly. For example, information that the government collects regarding a vulnerability in the community, such as those dealing with chemical plants or nuclear facilities, could relate to the threat of terrorist activity. Also, information about a chemical plant's risk management plan required to be submitted to EPA under the Clean Air Act could relate to the ability to interdict or disrupt terrorist activity or be considered information that would improve the response to a terrorist act.

Information that might be defined as homeland security information could include other required statutory or regulatory filings. Unlike the Critical Infrastructure Information (CII) subtitle, which drew substantial public attention because of its potential for heighten secrecy, this Sensitive But Unclassified provision has no savings clause that exempts the information from non-disclosure when it is required under statue or regulation by any agency. Moreover, this provision applies to all information submitted to the government, regardless of whether it was voluntary or not and regardless of what agency to which it was given.

Another definition that vastly expands the magnitude of these provisions' efforts to control information is the term "State and local personnel." In the subtitle many of the provisions specifically refer to sharing information with and restricting the use of information by state and local personnel, which includes entities such as governors, mayors, and state and local law enforcement. The definition also includes entities that seem to fall outside the typical notions of official state and local personnel.

> Sec. 892(f)(3) The term ''State and local personnel'' means any of the following persons involved in prevention, preparation, or response for terrorist attack:
>
> (A) State Governors, mayors, and other locally elected officials.
>
> (B) State and local law enforcement personnel and firefighters.

(C) Public health and medical professionals.
(D) Regional, State, and local emergency management agency personnel, including State adjutant generals.
(E) Other appropriate emergency response agency personnel.
(F) Employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal government in procedures developed pursuant to this section.

Including public health and medical professionals in the definition of state and local personnel has serious ramifications. While keeping them informed of potential problems and threats would make a great deal of sense, tying these professionals into a network of information secrecy and use restrictions, as these provisions may establish, could easily run counter to their responsibilities to protect their communities from and inform people about any health threats.

The final group in the definition – private sector entities that affect critical infrastructure -- essentially allows the federal government to incorporate anyone it wishes to identify. Like health and medical professionals, this has the potential to restrict the private sector's ability to use the information. Some have speculated whether this allows companies with critical infrastructure issues to arrange to give information to government if there is an agreement to categorize it as Sensitive But Unclassified.

Use Restrictions

The subtitle on information sharing specifies various restrictions on states and localities on the use and reuse of homeland security information, apparently including sensitive but unclassified information.

Sec. 892(b)(3) The procedures prescribed under paragraph (1) shall establish conditions on the use of information shared under paragraph (1)—
(A) to limit the redissemination of such information to ensure that such information is not used for an unauthorized purpose;
(B) to ensure the security and confidentiality of such information;

Thus, even if the Sensitive But Unclassified information is shared with a state or local government, the federal government can tell the recipient how they can handle such information. In the example above, it is possible that information about dangers posed by chemical plants collected through risk management plans might be shared with emergency planners, but they might be restricted from sharing that information with others in the community. These use restrictions are certain to create a significant chilling affect on the media's ability to obtain information on homeland security and related topics upon which the public has a right to be informed.

The main control mechanisms to enforce the restrictions on use of information among the state and local personnel are nondisclosure agreements. While the provisions also outline other actions such as issuing security clearances, declassifying information, and redacting releases, these appear to relate primarily to classified homeland security information. The nondisclosure agreements are recognized as the primary method for controlling Sensitive But Unclassified homeland security information.

Sec. 892(c)(2)(B) With respect to information that is sensitive but unclassified, entering into nondisclosure agreements with appropriate State and local personnel.

There is no way to know how restrictive these agreements of non-disclosure will be or if individuals will have much choice in signing them. Considering that the provisions extend to include health and medical professionals, and other private sector employees, it is possible that signing a nondisclosure agreement may become necessary just for one to keep their job. One thing certain -- the number of nondisclosure agreements will be large, and a huge management task for government. The law requires each federal agency to identify a designated official to be responsible for these issues.

Control by the Administration

This subtitle grants full responsibility and control over establishing policies and procedures to manage and share homeland security information, both classified and sensitive but unclassified, to the President.

> Sec. 892(a)(1) The President shall prescribe and implement procedures under which relevant Federal agencies—

Since the legislation does not assign an agency to establish the procedures, it is uncertain which agency will have responsibility for prescribing the procedures. The administration could use a presidential executive order or instruct the Office of Management and Budget or another office in the Executive Office of the President to issue a government-wide directive or bulletin. There is no certainty that the administration will allow public comments on these procedures or follow traditional regulatory methods. It appears the approach used for establishing the procedures is entirely at the President's discretion.

Whatever means the President uses to establish these procedures the choices made will affect all agencies. Provisions in the subtitle specifically require that the procedures and systems, once established, apply to all agencies.

> Sec. 892(a)(2) The President shall ensure that such procedures apply to all agencies of the Federal Government.

While this entire subtitle is supposed to be about encouraging and increasing the sharing of information between the federal, state and local authorities, the provisions may create the opposite effect.

> Sec. 892(c)(1) The President shall prescribe procedures under which Federal agencies may, to the extent the President considers necessary, share with appropriate State and local personnel homeland security information that remains classified or otherwise protected after the determinations prescribed under the procedures set forth in subsection (a).

The President has the right to determine who among states and localities needs the information, proposing to share the information "to the extent the President considers necessary." This need to know attitude is amplified by the limits that can be placed on use and reuse, described above.

The law does require the President to submit a report to Congress by November 25, 2003, one year after enactment, on the implementation of these new requirements. The report is to include recommendations for "additional measures…to increase the effectiveness of sharing of information between and among Federal, State, and local entities." The President is also to

recommend additional appropriations requests. The key oversight committees are the Senate and House Judiciary Committees and the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence.

Conclusion

Unfortunately, this troubling provision was enacted without debate in Congress or public scrutiny. Now signed into law the key will be to remain vigilant to the implementation of this new Sensitive But Unclassified requirement, which may arise through almost any means at the administration's disposal. At the very least, this subtitle provides the legislative justification for the ongoing efforts by OMB to define "sensitive but unclassified" information. At worst, they could be used to develop, with no public input, a system of secrecy that creates yet a new category of information beyond those considered classified and those exempt under the Freedom of Information Act. This is a most disturbing provision and has significant implications for those concerned about an open government. It calls for significant congressional oversight.