Response to Secretary of Commerce "Set of Incentives" for NIST RFI: "Developing a Framework to Improve Critical Infrastructure Cybersecurity"

Submitted by
Gary W. Fresen
2540 Violet Street
Glenview, Illinois 60026
Comments and Opinions in this Response are Personal and not related to my employer.
Contact Information:
Personal Email: gfresen1@gmail.com
Work Email: gary.fresen@zurichna.com
Work Phone: 312-775-9754

Federal Register, Vol. 78, No. 60, Thursday, March 28, 2013
The President has directed the Secretary of Commerce to evaluate a set of incentives designed to promote participation in a voluntary program to be established by the Secretary of Homeland Security to support the adoption by owners and operators of critical infrastructure and other interested entities of the Cybersecurity Framework being developed by the National Institute of Standards and Technology (NIST).

Proposal for Incentive

Legislation - Legal Privilege for Risk Analysis Assessment of Information Systems

Information Sharing is a critical issue for CyberSecurity. The success of Information Sharing, however, depends upon the creation of robust information at the grass roots level of individual Private Sector company network operations. Applying the well-known Information Technology notion of "Garbage In, Garbage Out," Information Sharing will only be effective if the information is worth sharing.

In my opinion, this key issue "creation of robust information" has not been adequately investigated or discussed by Congress during last year's CyberSecurity legislative efforts or by the President's advisors resulting in the recent Executive Order. Rather, the focus has been directed to the logistics and technical specifications of sharing data, but not on the development of useful information in the first instance.

Without robust information, the result of "sharing" over the past decade has been less effective than it could have been. NIST can develop a Framework to Improve Critical Infrastructure Cybersecurity, but the result of Information Sharing will not reach the desired goal of making our nation safer because the information that will be shared will not be robust enough. The Private Sector must perform more and better Risk Analysis Assessments of its networks and information systems.

As an attorney, I served on the American Bar Association Committee for Information Security, known as the Digital Signature Committee, in the 1990's and participated in discussions with Congressional staffers for Federal Legislation, which resulted in the last Information Sharing legislation in 2001. I participated in limited ways in the early days of the creation of ISACs and the FBI information sharing programs.

Because the focus of CyberSecurity discussions recently as well as over the last decade has been almost exclusively devoted to the technical details of "how to share," the participants have not considered an existing and a very effective tool for the creation of robust information.

The tool is a legal privilege that would allow a confidential Risk Analysis Assessment of Private Sector CyberSecurity issues.

Excellent models of the tool of a legal privilege exist that demonstrate how to create robust information in Private Sector industries. For example, lawmakers at State and Federal levels have enacted legislation to share information about Healthcare, Transportation and Environmental Protection. Legislation of privileges has created robust information to improve patient care from dangers of disease and death, to improve safety of our highways and railroad crossings, and to protect our environment. The models all include a legal privilege enacted to protect the information that is submitted in the reports shared with governmental entities.

I recommend that the Secretary of Commerce reach out to the General Counsel for hospitals and learn from them about the legal privilege enacted in all 50 States that authorizes the Corporate Governance of medical facilities to perform confidential studies, such as Morbidity and Mortality studies in Illinois, e.g. Jenkins v. Wu, 102 Ill. 2d 468 (1984), and ask them why the legal privilege is so important to improving patient care. You will find that the existence of the legal privilege creates a frank and unfettered discussion among professionals that is not "chilled" by the fear of disclosure. Of significance, no immunity is given and no underlying information, such as patient charts, is hidden or protected from disclosure by governmental officials or personal-injury-contingent-fee lawyers. Discovery in medical malpractice cases are permitted full access to all medical records and depositions of all hospital personnel. Only the confidential report, as limited by a State statute, is protected from discovery.

Consider the opportunity for CyberSecurity: If a hospital can perform a privileged risk analysis of its operations, such as locating a virus that is endangering patients, then the Private Sector should have a similar privilege under law to investigate viruses and other attacks that pose CyberSecurity threats.

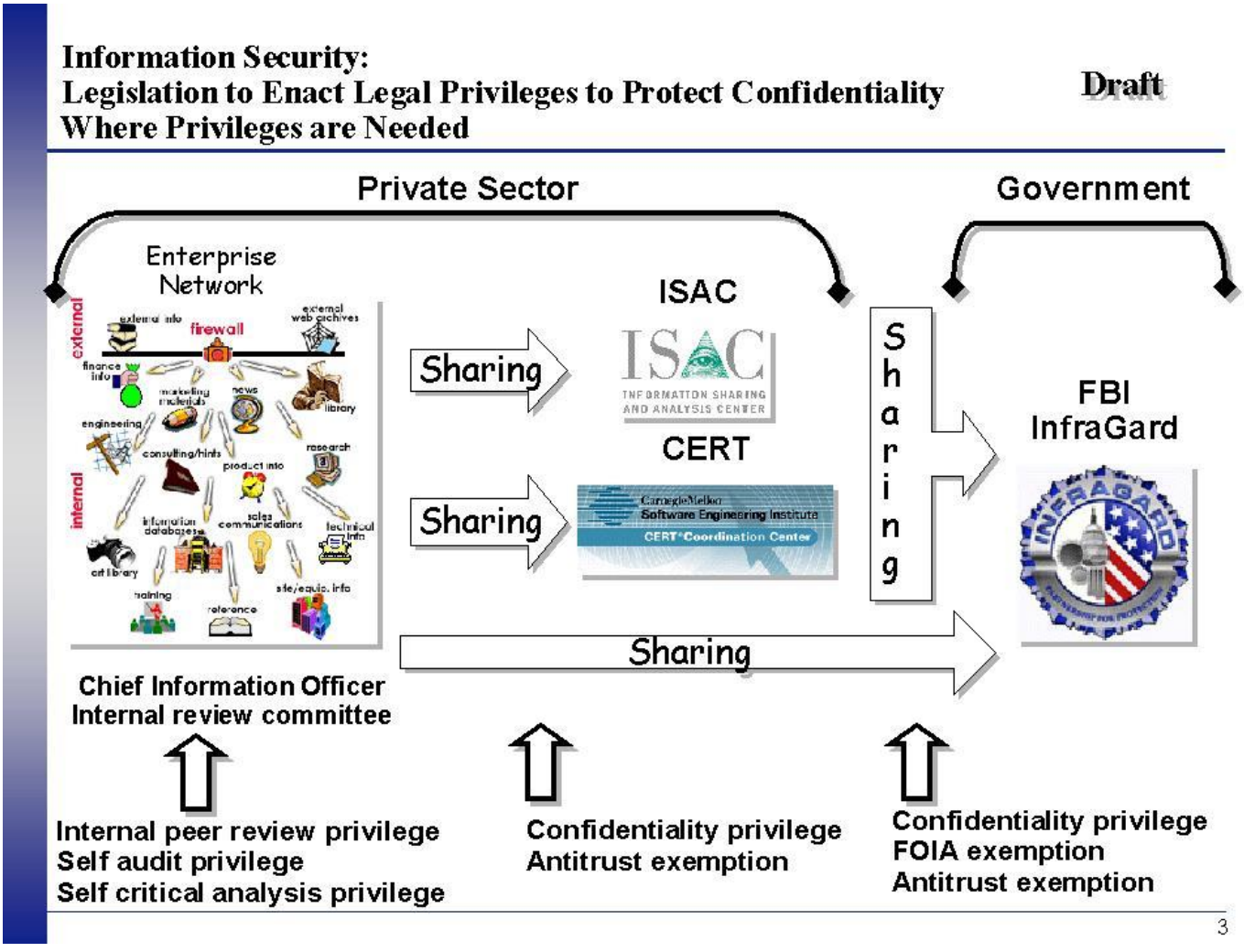
I also recommend that the Secretary reach out to the General Counsel of the major railroads or the Department of Transportation and ask them about the confidential reports about accidents at railroad crossings that are provided to the Department of Transportation. See, 23 U.S.C. 409 The reports result in robust information about the most dangerous crossings so that the Department of Transportation can identify where to spend the millions of dollars that are designated each year to eliminate safety hazards on our highways and roads. The Federal legal privilege for railroads creates reliable and robust information.

In conclusion, a legal privilege is an excellent incentive that should be created for CyberSecurity to allow the Private Sector to perform the important task of Risk Analysis Assessment of networks and information systems. Overlooking the incentive of a legal privilege in order to create robust information for sharing was a glaring weakness in the Federal legislative discussions and has not been given sufficient priority in the Administration's Executive Order. The Framework to Improve Critical Infrastructure Cybersecurity must consider the successful track record of a Self-Critical Analysis legal privilege.

Sincerely,
SS/ Gary W. Fresen

REFERENCE MATERIALS

Presentation in the 2001
Comments on pending Federal Legislation: House (106th) **HR 4246 Cyber Security Information Act** (Davis, VA) and Senate (107th) **S. 1456 Critical Infrastructure Information Security Act of 2001** (Bennett, UT)



From 2001 - Using the language of Senate Bill **S. 1456 Critical Infrastructure Information Security Act of 2001** (Bennett), I recommend adding a new section that creates the two categories of legal privileges:

New Section 5 added to Senate Bill S. 1456
SEC. 5. PROTECTION OF INTERNAL QUALITY REVIEW ORGANIZATION

(a) PROTECTION --
(1) IN GENERAL. —Notwithstanding any other provision of law, all information, documents, interviews, reports, statements, memoranda, recommendations, or other data of any person, organization, Information Sharing and Analysis Organization or its members, or other entity used in the course of:

(A) gathering and analyzing critical infrastructure information in order to better understand security problems related to critical infrastructure and protected systems, and interdependencies of critical infrastructure and protected systems, so as to en- sure the availability, integrity, and reliability of critical infrastructure and protected systems;
(B) communicating or disclosing critical infra- structure information to help prevent, detect, mitigate, or recover from the effects of a problem related to critical infrastructure or protected systems; or
(C) voluntarily disseminating critical infrastructure information to entity members, Information Sharing and Analysis Organizations, the Federal Government, or any entities which may be of assistance in carrying out the purposes specified in paragraphs (A)and (B),

may not, without written consent, be used by any person, entity, agency, any other Federal, State, or local authority or other government, or any third party, in any civil action arising under Federal or State or other law, unless such information is created or submitted in bad faith; and may not, without written consent, be used for a purpose other than the purpose of this Act.

* * * * * * *

http://faculty.nps.edu/dedennin/publications/it%20and%20security%20-%20grave%20new%20world.pdf

Information Technology and Security

Dorothy E. Denning
Georgetown University

One of the challenges facing all of these groups is that industry has been reluctant to share information out of concern for its confidentiality. In particular, companies are concerned that sensitive information provided voluntarily might not be adequately protected, or that it could be subject to Freedom of Information Act (FOIA) requests or lawsuits. Industry is also concerned that cooperation with industry partners might violate antitrust laws. Bills have been introduced in the House and Senate to provide limited exemption from FOIA and antitrust laws, but they might not go far enough. Gary Fresen, an attorney working on information security issues, recommends giving companies a broader range of legal privileges consistent with that found in other industries such as healthcare, railroads, and environmental protection. In addition to FOIA and antitrust protection, the privileges would include a peer group privilege, a self-audit privilege, and a reporting privilege. Collectively, these would protect company sensitive information that is acquired during vulnerability testing or that is shared with industry groups from disclosure through lawsuits.

* * * * * * *

Legal Privileges in Healthcare Industry

The Healthcare Industry's business model for on-going internal self-evaluation is particularly well-suited for adoption by the Information Security Industry in order to protect the nation's Critical Information Infrastructure.

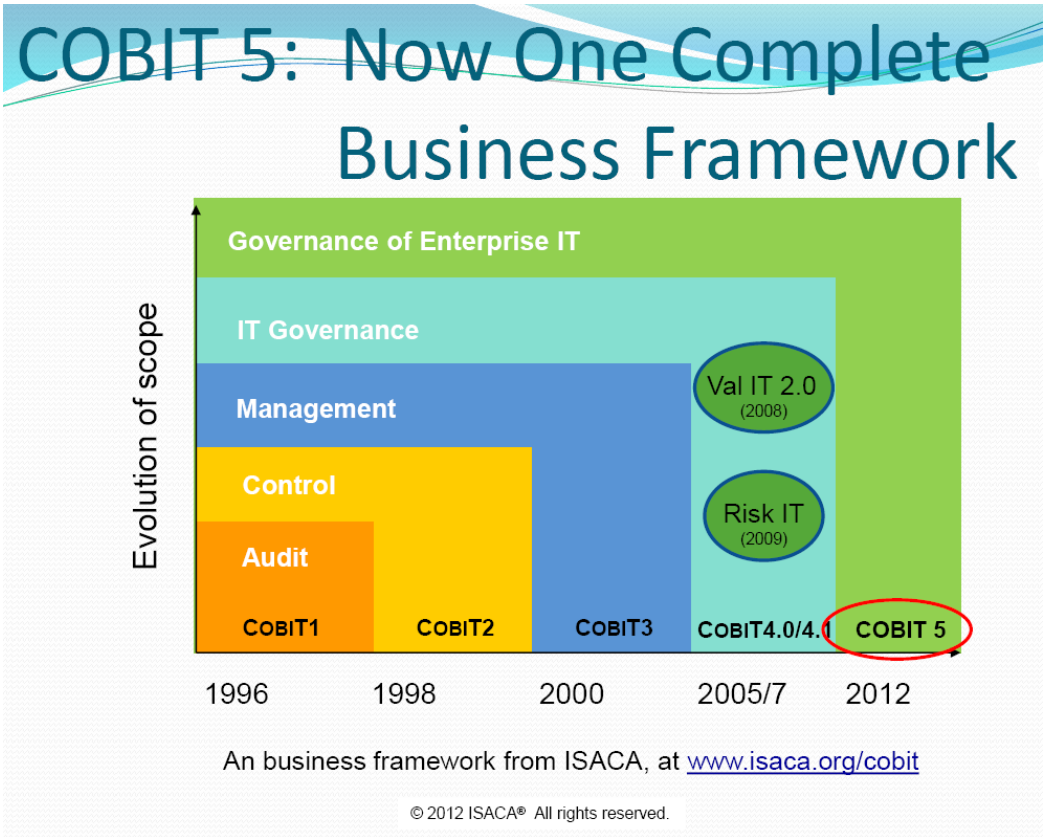
To illustrate, the management of a hospital includes regular meetings of "internal review committees" comprised of doctors and hospital personnel to evaluate the quality of health care provided by their institution. Specific operational policies and procedures are authorized by the hospital management to carry the administration of the internal institutional committees. The protection of the confidentiality of these activities plays an essential role in the delivery of quality services in the Healthcare Industry. I offer quotes from just three State Supreme Courts to demonstrate this principle:

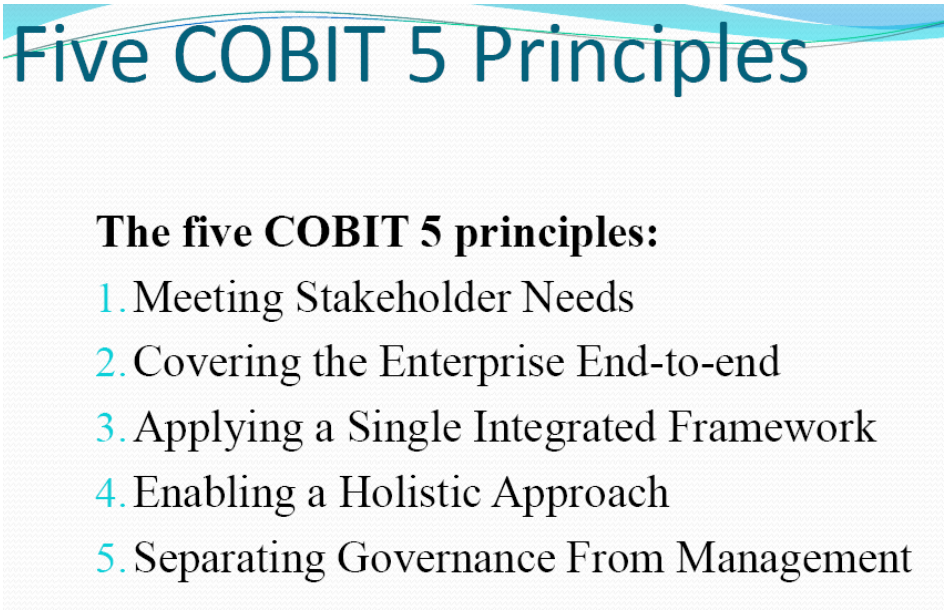
> The Illinois Supreme Court stated that the purpose of Illinois' Medical Studies Act is "to ensure the effectiveness of professional self-evaluation, by members of the medical profession, in the interest of improving the quality of health care" and noted that "the majority of State legislatures have passed legislation in the area of hospital-committee confidentiality." Jenkins v. Wu, 102 Ill. 2d 468 (Ill. 1984)
>
> The Minnesota Supreme Court concluded that the statutes providing for confidentiality and immunity for peer review organizations and persons involved in the peer review process reflect a legislative intent both to improve the quality of health care by providing for confidentiality of review organization information and to encourage self-monitoring in the medical profession. Kalish v. Mount Sinai Hosp., 270 N.W.2d 783 (Minn. 1978)
>
> The South Carolina Supreme Court explained: "'The overriding public policy of the confidentiality statute is to encourage health care professionals to monitor the competency and professional conduct of their peers to safeguard and improve the quality of patient care. The underlying purpose behind the confidentiality statute is not to facilitate the prosecution of civil actions, but to promote complete candor and open discussion among participants in the peer review process. ..." "'We find that the public interest in candid professional peer review proceedings should prevail over the litigant's need for information from the most convenient source." McGee v. Bruce Hosp. System, 312 S.C. 58, 439 S.E.2d 257 (1993)

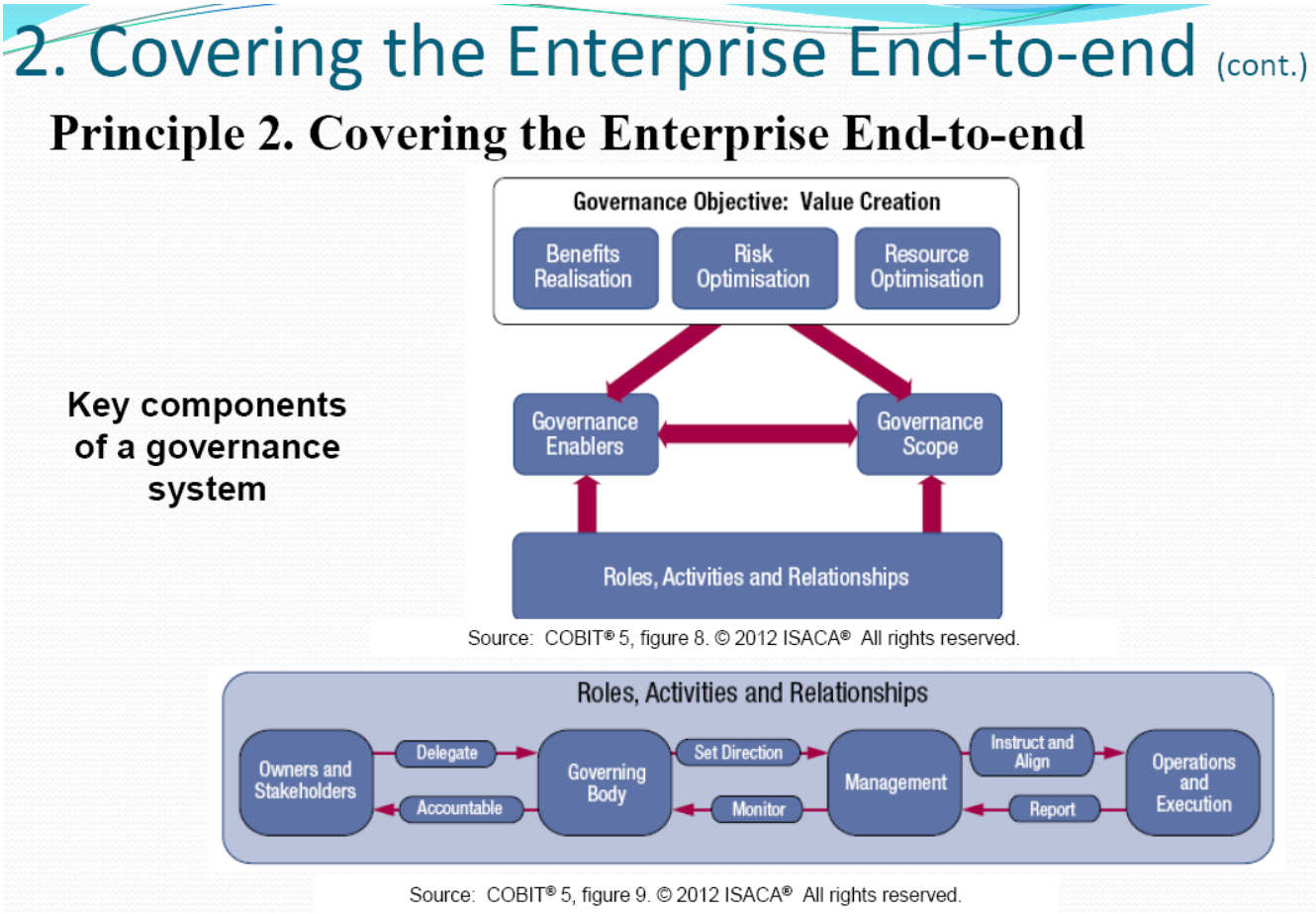
The Healthcare model, by asserting a privilege for risk assessment, monitoring and reporting, fits well with the principles of Information Security. A good example of this fit is to compare the Healthcare model with the standards of IT Governance and the COBIT Information Security Program that have been prepared for the Accounting Profession by the Information Systems Audit and Control Association (ISACA). See http://www.isaca.org/. (COBIT refers to "Control Objectives for Information and related Technology).

* * * * * * *

Corporate Governance of Enterprise Information Technology: COBIT recommendations:







* * * * * * *

Legal Privileges in Transportation Industry

Washington Law Review, July, 2002
77 Wash. L. Rev. 951
NOTES & COMMENTS: REVERSE PRESUMPTIONS:
GUILLEN V. PIERCE COUNTY DISREGARDS REASONABLE CONSTITUTIONAL INTERPRETATIONS OF 23 U.S.C. § 409 - United States Supreme Court, 537 U.S. 129 (2003)

I. FEDERAL AND STATE LAWS REQUIRE COLLECTION OF HIGHWAY DATA

Federal funding programs, enacted to improve national highway safety, require participating states to report highway data and maintain engineering surveys. n17 The surveys may utilize highway data whose collection is also required by Washington State statutes and regulations. n18 Section 409 creates a privilege for highway data collected for certain federal programs, preempting state discovery rules. n19

A. Federal Highway Safety Programs Require Comprehensive Data Collection

Introducing its first major highway safety initiative in 1966, Congress reported that more Americans had died on the country's highways than in all its wars combined; in 1965 alone, highway accidents caused 49,000 deaths. n20 In response to a finding that inadequate research,

resources, and national coordination had been devoted to this problem, the Highway Safety Act of 1966 directed states to develop comprehensive programs to reduce traffic accidents, in conformity with federal standards. n21 The 1966 Act provided funding and established standards for training and education, vehicle inspection, highway design and surveillance systems, and accident record-keeping systems. n22 It also directed states to collect and report such data as the federal government required. n23

Since 1966, Congress has expanded federal highway safety funding to cover actual roadway improvement projects and has correspondingly increased data collection requirements. n24 In 1973, reporting that highway deaths had climbed to 56,000 in 1972 and threatened to rise to 80,000 by 1980, n25 Congress established several ongoing safety enhancement funding programs for hazard elimination, n26 railroad crossings, n27 and highway bridge projects. n28 Extensive evaluation and reporting requirements accompanied these programs. n29

* * *

C. Section 409 Was Enacted to Mitigate Litigation Impact of Federally-Required Recordkeeping

In 1987, recognizing that state compliance with federal safety programs made additional evidence available to tort plaintiffs, n45 Congress enacted 23 U.S.C. 409. n46 Prior to its amendment in 1995, 409 provided that:

> Notwithstanding any other provision of law, reports, surveys, schedules, lists, or data compiled for the purpose of identifying, evaluating, or planning the safety enhancement of potential accident sites, hazardous roadway conditions, or railway-highway crossings, pursuant to sections 130, 144 and 152 of this title or for the purpose of developing any highway safety construction improvement project which may be implemented utilizing Federal-aid highway funds shall not be subject to discovery or admitted into evidence in a Federal or State court proceeding or considered for other purposes in any action for damages arising from any occurrence at a location mentioned or addressed in such reports, surveys, schedules, lists, or data. n47

While agreeing that 409 has no legislative history, n48 courts have consistently inferred two purposes for the legislation. n49 First, Congress sought to prevent federal record-keeping requirements from creating an additional piece of ready-made evidence for private litigants. n50 Second, Congress wanted to encourage the "free flow" of safety information n51 and the candid evaluation of local safety hazards. n52 Permitting governments to obtain safety information "free from the fear of future tort actions" n53 has been said to promote the federal government's interest in obtaining complete and accurate highway information n54 and ensuring deliberative spending of federal funds. n55

Section 409 expressly preempts state laws and court rules that would allow plaintiffs to obtain and use some government highway data in tort cases, n56 but the privilege has not been construed to grant governments complete immunity from negligence suits. n57 Though legislation enacted pursuant to Congress' constitutional authority preempts inconsistent state laws, n58 state tort systems have continued to operate alongside federal transportation safety schemes. n59 Section 409's impact on state tort systems depends upon how broadly courts construe its preemptive scope. n60

* * * * * * *

Governance of Enterprise Security: CyLab 2012 Report
How Boards & Senior Executives Are Managing Cyber Risks
Author: Jody R. Westby, Adjunct Distinguished Fellow, CyLab CEO, Global Cyber Risk LLC
May 16, 2012

RECOMMENDATIONS

The survey revealed that governance of enterprise security is still lacking in most corporations, with gaps in critical areas. If boards and senior management take the following 12 actions, they could significantly improve their organizations' security posture and reduce risk:

1. Establish a board Risk Committee separate from the Audit Committee and assign it responsibility for enterprise risks, including IT risks. Recruit directors with security and IT governance and cyber risk expertise.
2. Ensure that privacy and security roles within the organization are separated and that responsibilities are appropriately assigned. The CIO, CISO/CSO, and CPO should report independently to senior management.
3. Evaluate the existing organizational structure and establish a cross-organizational team that is required to meet at least monthly to coordinate and communicate on privacy and security issues. This team should include senior management from human resources, public relations, legal, and procurement, as well as the CFO, the CIO, CISO/CSO, CRO, the CPO, and business line executives.
4. Review existing top-level policies to create a culture of security and respect for privacy. Organizations can enhance their reputation by valuing cybersecurity and the protection of privacy and viewing it as a corporate social responsibility.
5. Review assessments of the organization's security program and ensure that the program comports with best practices and standards and includes incident response, breach notification, disaster recovery, and crisis communications plans.
6. Ensure that privacy and security requirements for vendors (including cloud and software-as-a-service providers) are based upon key aspects of the organization's security program, including annual audits and control requirements. Carefully review notification procedures in the event of a breach or security incident.
7. Conduct an annual audit of the organization's enterprise security program, to be reviewed by the Audit Committee.
8. Conduct an annual review of the enterprise security program and effectiveness of controls, to be reviewed by the board Risk Committee, and ensure that identified gaps or weaknesses are addressed.
9. Require regular reports from senior management on privacy and security risks.
10. Require annual board review of budgets for privacy and security risk management.
11. Conduct annual privacy compliance audits and test incident response, breach notification, disaster recovery, and crisis communication plans.
12. Assess cyber risks and potential loss valuations and review adequacy of cyber insurance coverage.