AUDITED SELF-REGULATION IN PROPOSED CYBERSECURITY LEGISLATION

When a government decides to regulate the behavior of its citizens, it can choose among a wide variety of options. In a traditional police-state, a government would simply make it a crime to behave or not behave in a certain way. Democratic governments historically have used "command and control" regulation, in which the government creates specific obligations, enforceable by civil or criminal penalties, to regulate the behavior of their citizens.[1]

However, as social and economic conditions have become more complicated, so have the government's attempts to regulate behavior. Beginning in the 1960s, the U.S. government veered from the command and control approach in regulating different types of market failure.[2] The government began with "market-based" or "incentive-based" regulations and attempted to regulate behavior through incentives, sometimes combined with obligations.[3] The government also used the tax code as a way to regulate desired behavior through exclusions, deductions, credits, and preferential tax rates.[4]

The government can regulate outside incentives and punishments by creating new markets,[5] delegating regulatory authority,[6] educating the public directly,[7] creating partnerships with the private sector,[8] and forcing disclosure.[9] The government has attempted to regulate the security and cybersecurity of various industries using many of these methods.

The government is now focusing on audited self-regulation to regulate certain industries' behavior as it pertains to cybersecurity. By audited self regulation, we mean a governmental

---

1 Timothy F. Malloy, *Regulating by Incentives: Myths, Models, and Micromarkets*, 80 Tex. L. Rev. 531 (2002).

2 Douglas C. Michael, Federal Agency Use of Audited Self-Regulation As A Regulatory Technique, 47 Admin. L. Rev. 171, 186 (1995).

3 See, Malloy, supra, at 532.

4 Eric A. Lustig, The Emerging Role of the Federal Tax Law in Regulating Hostile Corporate Takeover Defenses: The New Section 5881 Excise Tax on Greenmail, 40 U. Fla. L. Rev. 789, 820 (1988).

5 See, Lesley K. McAllister, Beyond Playing "Banker": The Role of the Regulatory Agency in Emissions Trading, 59 Admin. L. Rev. 269, 270 (2007) (discussing the "cap and trade" market created by the government where the regulatory agency acts as an accountant and keeps track of trades while imposing penalties for noncompliance in this legislatively-created market of "cap and trade.").

6 See, Paul M. Architzel, The Role of Exchanges as Self-Regulatory Organizations in an Increasingly Competitive Landscape, 25 No. 5 Futures & Derivatives L. Rep. 1 (discussing various financial organization who are also self-regulatory organizations).

7 See, National Research Council. "Paper Contribution J: Legal and Public Policy Interventions to Advance the Population's Health." Promoting Health: Intervention Strategies from Social and Behavioral Research, Washington, DC: The National Academies Press, 2000.

8 See, Public-Private Partnerships and Insurance Regulation, 121 Harv. L. Rev. 1367, 1368 (2008) (discussing private-public partnerships).

9 See, Battle Escalates Over Forced Disclosure of Financial Records, 25 No. 8 Jud./Legis. Watch Rep. 3. (2004) (discussing possible legislation enacting criminal penalties on financial companies that fail to disclose certain records).

delegation of the power to implement public goals to nongovernmental entities subject to review by a federal agency, backed by a public audit of the private entities' performance. Audited self regulation permits the government to achieve regulatory goals by relying on the regulated entities to keep their own house in order. The resulting regulation likely is more flexible and designed to meet the specific circumstances at each firm affected.

Audited self-regulation can take several forms. In one form, the private self-regulatory organization (SRO), usually composed of members of the industry, can set regulatory standards and audit companies to ensure compliance. Typically in audited self-regulation, a government regulatory agency provides minimal monitoring of the SRO to ensure some level of efficacy. In another form of audited self-regulation, the regulatory standards are set by the governmental agency, and the only role for the SRO is auditing companies to ensure compliance.

The goals of this paper are to present a brief overview of audited self-regulation, suggest the factors that likely will determine when the approach will be successful, and then assess the likelihood of success for audited self regulation in the cybersecurity context.

PROPOSED CYBERSECURITY LEGISLATION

Cybersecurity is one of the most pressing issues facing the U.S. today. Our nation may be threatened more by disruption of our critical infrastructure than by traditional terrorist threats of bombing and mayhem. There is any number of ways to protect against cyber attacks. Traditional command and control regulation, for instance, is one option, mandating what steps industries must pursue to shield critical infrastructure from terrorist disruption. But Congress is also considering several bills that would use a system of audited self-regulation to help protect cybersecurity.

The Senate is currently considering two separate bills intended to protect the cybersecurity of U.S. critical infrastructure. In February 2012, Senators Lieberman and Collins introduced S 2105, "A Bill to Enhance the Security and Resilience of the Cyber and Communications Infrastructure of the United States" or the "Cybersecurity Act of 2012." In response, Senator McCain introduced S 2151, the "Strengthening Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012" or "SECURE IT." The House is also considering a bill itself, H.R. 3674, the "Precise Act."

All of the proposed bills address owners and operators of critical infrastructure and require them to share information with the federal government to protect against threats, especially cyber threats. The Cybersecurity Act of 2012 in addition utilizes audited self regulation as a tool to achieve cybersecurity. The proposed Act requires the Secretary of the Department of Homeland Security, in consultation with various private and public entities, to assess cybersecurity threats, vulnerabilities, and risks. Then, having identified the highest at-risk sectors, the Secretary will conduct cyber risk assessments of industries on a sector-by-sector basis. Based on these assessments, the Secretary designates certain assets or systems as "critical infrastructure" which will then be covered by the requirements of the act.

The Secretary can only designate an asset as critical infrastructure if damage or unauthorized access to that asset could reasonably result in (1) the interruption of life-sustaining services; (2) catastrophic economic damage to the U.S.; or (3) severe degradation of national

security or national security capabilities. Under these terms, the Secretary could reasonably designate as critical infrastructure assets within the water industry, the various power industries, and the financial industry as critical infrastructure. The Act does not permit the Secretary to designate as critical infrastructure any information technology product, hardware, or software based solely on a finding that the product or service is being used, or capable of being used, in covered critical infrastructure.

Then, in consultation with the various private and public entities, the Secretary will develop risk-based cybersecurity performance requirements. These requirements may be based on existing industry practices or by selecting and adapting requirements from existing ones or proposals. If the Secretary determines that none of the performance requirements satisfies the other provisions or purposes of the Act, the Secretary, in conjunction with the private and public entities, can develop new ones. At all times, the President can exempt an appropriate part of critical infrastructure from these requirements if he determines that a sector-specific regulatory agency has sufficient enforcement mechanisms already in place to mitigate risks.

Owners and operators of assets that have not been exempted by the President must annually certify that they have developed and effectively implemented security measures sufficient to satisfy the remaining provisions of the Act. They must also submit to a third party assessment of their security measures. Any owners or operators of covered assets who violate these requirements and then fail to remediate such a violation in a reasonable timeframe will have to pay civil fines.

The required third-party assessments must use reliable, repeatable, performance-based evaluation and metrics to assess the security measures. Owners or operators can only use third-party assessments that have been certified by the Secretary and undergo regular retraining and certification. The Cybersecurity Act protects the information gathered both in voluntary sharing and the annual certifications and assessments. Specifically, it protects any information that is a privileged or confidential trade secret or commercial or financial transactions.

HISTORY/CASE STUDIES

In order to understand what makes a program of audited self-regulation successful, this section examines the results of past audited self-regulation programs in the electricity, nuclear, and welding industries. Audited self regulation does not have uniform appeal across regulatory contexts.

Electricity

Electricity and the bulk power system currently are regulated under an audited self-regulation[10] scheme run by the North American Energy Reliability Corporation ("NERC"), whose rulemaking is subject to review by the Federal Energy Regulatory Commission ("FERC"). NERC is a nonprofit non-governmental organization made up of industry expert volunteers. The electricity industry began regulating itself in 1968 in response to widespread blackouts so that it could "develop and promote rules and protocols for ... reliable operation."[11] The bulk power industry is interconnected, and due to the nature of electricity, is only as strong as the weakest

---

[10] Douglas C. Michael, *Federal Agency Use of Audited Self-Regulation As A Regulatory Technique*, 47 Admin. L. Rev. 171, 176 (1995)

[11] North American Electric Reliability Corporation. Company Overview: History. http://www.nerc.com/page.php?cid=1|7|10

link. Despite voluntary regulation, the blackout of 2003 in the northeastern U.S.,[12] the worst in the nation's history, exposed reliability issues in the electricity grid. In 2005, Congress passed the Electricity Modernization Act, which amended the Federal Power Act[13] to require FERC to certify a self-regulatory organization, to be called the "Electric Reliability Organization." The existing nonprofit voluntary regulation organization, NERC, made up of industry experts,[14] was certified as the Electric Reliability Organization.[15] NERC oversees the interconnected public power systems in the United States, Canada, and part of Mexico. NERC is responsible for drafting, implementing, and enforcing critical infrastructure reliability standards. Standards promulgated by NERC are enforceable in the U.S. through civil penalties.

The electricity industry is an organized industry that has a natural incentive to promote reliability because all electricity companies are economically dependent on the "weakest link" in the grid. The industry is no stranger to regulation, but is also highly motivated to self-regulate in order to avoid more complete government regulation in the sector. NERC has maintained that it is independent and capable of regulating itself, often questioning what it claims to be a heavy-handed approach to oversight by FERC in the last several years, calling FERC a "Monday morning quarterback."[16]

Audited self-regulation has historically been appropriate in the electricity sector because safeguarding the reliability of the electricity grid requires expertise from the industry itself. In many ways, this audited self regulation scheme appears to be successful, although the relationship between FERC and NERC has become strained several times. One continuing issue is that the role of FERC in the self-regulatory scheme is somewhat unclear. Although often deferring to NERC, FERC has notably remanded standards in several key instances, creating confusion and debate about what the proper role of each agency should be.[17] In most of these cases, FERC required more stringent standards because of what it identified as "reliability gaps."[18] This robust dialogue about how best to protect the bulk power system indicates that the scheme is not toothless and also that NERC is not as autonomous as the industry would like.

---

12 For a technical background on how the August 14, 2003 blackout started and ultimately cascaded across the northeast United States and Ontario, See http://www.nerc.com/docs/docs/blackout/ch5.pdf.

13 §215 Section 215 requires FERC to certify an Electric Reliability Organization to develop mandatory and enforceable Reliability Standards, which are subject to Commission review and approval. Once approved, the Reliability Standards may be enforced by the ERO, subject to Commission oversight, or the Commission can independently enforce Reliability Standards. 16 U.S.C. 824o(e)(3) (2000 & Supp. V 2005)

14 NERC includes committees and subcommittees of industry experts and stakeholders, and approximately 1,400 registered entities who are affected by the regulations. http://www.nerc.com/page.php?cid=1|9

15 3779 PUR Util. Reg. News 6

16 23-WTR Nat. Resources & Env't 61

17 In Order No. 683, FERC declined to defer to NERC's reliability standards in all cases, arguing that ". . . simply because a proposed Reliability Standard has been developed through an adequate process does not mean that it is adequate as a substantive matter in protecting reliability. We will, therefore, review each Reliability Standard to ensure that the Reliability Standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest, giving due weight to the ERO." John S. Moot, *When Should the Ferc Defer to the Nerc?*, 31 Energy L.J. 317, 321 (2010)

18 4040 PUR Util. Reg. News 1

Nuclear

After the Three Mile Island disaster in 1979, the Institute for Nuclear Power Operations (INPO) was created. Strong federal regulation by the Nuclear Regulatory Commission (NRC) and an immediate threat of legislation imposing strict government oversight of nuclear plants, or possibly even closing them down, served as a powerful catalyst for the creation of INPO.[19] INPO is a private, industry wide regulatory body whose official mission is to "promote the highest levels of safety and reliability –to promote excellence- in the operation of commercial power plants."[20] INPO developed standards on how the agency should be policed. NRC adopted the standards, and meeting these standards became a prerequisite of getting an initial or continuing license from NRC.[21] NRC's willingness to defer to INPO was challenged by the D.C. Circuit, which found that the NRC had failed to comply with the statutory directive that NRC "promulgate regulations, or other appropriate guidelines, for the training and qualifications of civilian nuclear power plant personnel."[22] The statute did not permit NRC simply to issue policy statements, but rather required NRC to promulgate mandatory instructional requirements for training programs.[23] Thus NRC was forced to create final rules of its own that directly mandate training program standards and provide instructions on how to comply with them.[24] The NRC's Office of the Inspector General (OIG) was established on April 15, 1989, as an independent and objective unit to conduct and supervise audits and conduct investigations relating to NRC's programs and operations.[25]

Rees (1994) notes that the Institute of Nuclear Power Operation (INPO) is successful because it is able to support its internal sanctions through a threat to reveal non-compliance to the Nuclear Regulatory Commission.[26] Anything identified by peer review that is not acted upon in timely fashion is referred to the INPO governing body of all the utility CEOs. The strong peer pressure to maintain high standards is reinforced by INPO giving each plant a rating on one of four levels that directly affects insurance premiums. INPO has strong ties with the World Association of Nuclear Operators (WANO), acting as WANO representative on US soil, and its

---

19 Saule T. Omarova, Wall Street As Community of Fate: Toward Financial Industry Self-Regulation, 159 U. Pa. L. Rev. 411, 452 (2011)

20 About Us, Inst. of Nuclear Power Operations, http:// www.inpo.info/AboutUs.htm

21 Commission Policy Statement on Training and Qualification of Nuclear Power Plant Personnel, 50 Fed. Reg. 46,603 (1988)

22 42 U.S.C. Sec. 10226 (1988)

23 Pub. Citizen v. Nuclear Regulatory Comm'n, 901 F.2d 147 (D.C. Cir. 1990)

24 Training and Qualification of Nuclear Power Plant Personnel, 58 Fed. Reg. 21, 904, 21,908 (1993).

25 Homepage of NRC's OIG, available at http://www.nrc.gov/insp-gen.html (last accessed April 26, 2012)

26 REES, J. (1994). Hostages of Each Other: The Transformation of Nuclear Safety since Three Mile Island. Chicago: University of Chicago Press. Quoted in The Oxford Handbook of Business and the Natural Environment (Oxford Handbooks) [Hardcover] Pratima Bansal (Editor), Andrew J. Hoffman (2012) p111.

staff often have key positions as Team Leaders or Assistant Team Leaders in WANO peer reviews.[27]

In testimony before the BP Deepwater Horizon Oil Spill and Offshore Drilling Commission in August 2010 the CEO of INPO said, "[I]ndustry self□regulation has been one driving factor toward improved industry performance. In the early 1980s, the typical nuclear power plant had a capacity factor of 63 percent, experienced seven automatic shutdowns per year, and had collective radiation exposure levels that could be significantly reduced. Today, the typical plant has a 91 percent capacity factor with zero automatic shutdowns per year and an occupational radiation exposure about six times lower than in the 1980s."[28] And in its final report, the commission put in place to investigate the oil spill backed the creation of an industry-run organization modeled on INPO.[29]

Through a mix of communication, education, and peer-pressure, Rees suggests that INPO has managed to secure a high level of commitment within the nuclear power industry to self-regulate.[30] The small size of the nuclear industry may be one reason for this success: the industry is made up of only 54 different utilities and 104 nuclear plants at 70 different sites.[31] A second important factor is that the nuclear industry faces much less competition than do other industries. Nuclear power plants compete with fossil fuel plants but rarely with each other (although this is changing as a result of deregulation in some states such as California).[32] And third, the nuclear industry is relatively homogeneous: technologically, most nuclear power plants are very similar to one another.[33] All of these factors have contributed to the success of a system of audited self-regulation in the nuclear industry.

Welding Industry in New Zealand

New Zealand's welding industry offers a look at the potential pitfalls of audited self-regulation. In 1992, New Zealand instituted a broad scheme of audited self-regulation of the health and safety of all employees. The Health and Safety in Employment Act did not set up top-down command and control regulations, but instead instituted a system of audited self-regulation scheme for all employers. In broad terms, the Act required employers to create and maintain safety standards for employees and empowered governmental auditors to sanction non-complying businesses.

The Act governs any "person who or that employs any other person to do any work for hire or reward."[34] Using broad language, the Act requires all employers to identify hazards, eliminate or isolate hazards, train and supervise employees, and develop emergency procedures.

---

27 http://www.world-nuclear.org/info/inf38.html

28 http://www.world-nuclear.org/info/inf38.html

29 http://www.washingtonpost.com/wp-dyn/content/article/2011/01/10/AR2011011007093.html

30 REES, J. (1994). Hostages of Each Other: The Transformation of Nuclear Safety since Three Mile Island. Chicago: University of Chicago Press.

31 statistics available at http://www.nei.org/resourcesandstats/nuclear_statistics/usnuclearpowerplants/

32 *Id*

33 *Id.*

34 Health and Safety in Employment Act of 1992, Part 1, Section 2 "Interpretation." http://legislation.govt.nz/act/public/1992/0096/latest/whole.html#dlm279669

The Act allows government inspectors to audit compliance with the Act and issue notices of improvement or prohibition. Notices of prohibition require an employer to cease an activity. Failure to comply with notices can be punished with fines up to $10,000 under the Act. Employers who knowingly put employees at a reasonably likely risk of serious harm can face up to two years imprisonment, a fine of up to $50,000 or both.[35] The Act authorizes the creation of additional agencies and regulations to ensure compliance, although such agencies have not been developed in every sector. In the welding industry, the Act's directive to create regulations falls directly on each individual employer. No intermediary trade group exists that is charged with creating regulations for the industry as a whole.

Five years after the Act went into effect, an audit of safety conditions in the welding industry measured the effectiveness of the Act. The results were not encouraging. The audit revealed that over half of New Zealand welders had not even adopted hazard identification, one of the basic safety procedures required by the Act.[36] Sixty-eight percent of companies had not undertaken any staff training.[37] Following the audit, commentators suggested that one reason audited self-regulation failed in the welding industry was the small size of most welding companies: the average New Zealand welding company has fewer than 6 employees.[38] The commentators opined that small companies may have had difficulty developing safety standards and assessing compliance. Several have requested the New Zealand Department of Labour to "return to more specific exposition of expected workplace standards."[39]

In response, the New Zealand government attempted to improve the Act. In 2002, the government added harsher penalties for noncompliance, including an increased fine and even potential imprisonment. However, the Act's problems in practice did not lead the government to abandon audited self-regulation. Instead of moving toward a command and control regulation scheme, the Department of Labour published an extensive manual on Health and Safety in Welding Best Practices in 2006.[40] These best practices are not regulations, but may serve as guidance to small companies that are struggling to create adequate safety measures on their own. In more organized industries, the role of creating best practices might instead be taken on by a trade group.

Audited self-regulation has been unsuccessful in the New Zealand welding industry. The small size of the industry, the lack of an intermediary trade group with the resources to create regulations, and the bottleneck of too few governmental auditors have all contributed to the problems of audited self-regulation in this case.

---

35 *Id.* at Section 49 "Offenses likely to cause serious harm."

36 C.B. Walls and E.W. Dryson, Failure after 5 years of self-regulation: a health and safety audit of New Zealand engineering companies carrying out welding, 52 Occup. Med. 305, 305 (2002). http://occmed.oxfordjournals.org/content/52/6/305.full.pdf

37 *Id.* at 306.

38 *Id.* at 307.

39 *Id.* at 308.

40 http://www.osh.govt.nz/order/catalogue/pdf/welding-dol10157.pdf

DETERMINANTS OF SUCCESSFUL AUDITED SELF-REGULATION

The above case studies suggest that a number of identifiable factors bear on whether a program of audited self-regulation is likely to be successful. The following factors are highly relevant: (1) fear of government takeover/inevitability of regulation, (2) need for specialized knowledge, (3) alignment of natural private sector incentives with government regulatory interests, (4) ability and willingness of regulatory agencies to audit. This section discusses these factors in an attempt to create a framework for analyzing the probability of success of proposed systems of audited self-regulation, as under the proposed Cybersecurity Act of 2012.

Inevitability of regulation

All other things being equal, an industry facing a significant threat of "takeover" by a government regulatory agency intent on instituting "command and control" regulation will have a greater incentive to create a meaningful system of audited self-regulation. In other words, when regulation of some kind is inevitable, industry will work harder to create a system of audited self-regulation.

This threat of takeover often results from a large disaster and the subsequent public outcry for greater regulation. For example, the Three Mile Island disaster helped to rally the nuclear industry and made a very strong case for self-regulation. One author notes that, after Three Mile Island, "the nuclear power industry developed a strong sense that its very existence would be seriously threatened if another accident occurred and public pressure for 'safer alternatives' forced the government to shut down nuclear plants."[41] The subsequent system of audited self-regulation in the nuclear power industry was very successful. In the chemical industry, the Bhopal disaster in India galvanized the industry to implement a self-regulatory system designed to prevent a future disaster.[42] For both the chemical industry and the nuclear industry, the goal of both industry and government is the same: to prevent another disaster.

In industries like these, companies recognize that significant regulation is inevitable and the only question is the form the regulation should take. And if the companies see command and control regulation as potentially harmful, the motivation to make audited self-regulation work is increased. Such a disaster would be bad for the industry's image and business, and the government has a natural interest in protecting its citizens.

Still, the possibility of a disaster does not always mean that the interests of industry will be aligned with government regulatory interests. Although no lives were lost, the financial collapse of 2008 was a disaster in its own right. But the continued presence of a government willing to "bail out" struggling financial companies in case of a crisis "is one of the key--and unique--factors undermining any impulse for collective self-restraint of risk-seeking behavior."[43] In other words, even though the private sector shares the government's concern with preventing cyber attacks on the financial industry, the concern is muted by the potential for government bailouts for too-big-to-fail companies. Thus, the government's regulatory interest and the interests of the industry are not aligned, and audited self-regulation has been less successful in the financial industry.

---

41 Omarova at 454.

42 John Braithwaite, *The Regulatory State?* In Robert E. Goodin, ed., *The Oxford Handbook of Political Science* (2011) at 230.

43 Omarova at 480-481.

Where regulation is not inevitable, there is less motivation to implement a self-regulatory system. For example, the field of social networking is lightly regulated, and regulation in the area does not seem imminent.[44] In short, companies with no threat of disaster or inevitable regulation have less reason to commit to an effective program of audited self-regulation.

Need for specialized knowledge

The greater the need for specialized knowledge of an industry in order to regulate it, the greater the likelihood of success of a program of audited self-regulation. When it would be prohibitively expensive for a regulatory agency to acquire enough expertise to regulate an industry, audited self-regulation makes sense. This is true in industries like electricity, where specialized knowledge from the industry is essential in order to properly regulate the system. In the electrical industry, NERC has been a critical part of the regulatory system. As one commentator put it, "It is more efficient for government to rely on [industry's] collected expertise than to reproduce it at the agency level.[45] Similarly, when the pace of technological progress is particularly acute, government regulators may not be able to keep up. Thus, audited self-regulation presents a potential solution to one of the central questions facing the modern administrative state: how to keep track of the vast amounts of information necessary to regulate a complex modern industry without resorting to overbroad rules that can cripple the industry.

Alignment of private sector interests and government

If the firms in an industry have similar interests and incentives, and the industry already relies on self-regulating organizations or trade associations, audited self-regulation is more likely to be successful. But the level of organization and cooperation among companies varies widely in different industries. This could be a result of the size and heterogeneity or homogeneity of the industry: a large, heterogeneous industry, akin to the welding industry, is less likely to feature a "community of fate" mentality than a small, homogeneous industry.[46] In addition, larger industries will be more likely to face a "free rider" problem, whereby companies can benefit from the regulatory efforts of other companies without paying any costs themselves.

In the electricity industry, the interests of private companies are aligned and the industry is relatively well organized. In other words, the electricity industry has a strong "community of fate" mentality that promotes cooperation and organization within the industry.[47] This is largely because the interconnected nature of the electricity grid means that the entire system is only as strong as its weakest link. This increases the likelihood of success of an audited self-regulation program because companies recognize that cooperation is in their own best interests.

The experience of the nuclear industry also suggests that more organized industries with fewer participants are more likely to have successful programs of audited self-regulation. As

---

[44] Despite some urging to the contrary. *See e.g.*, Lori Andrews, *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy* (2012).

[45] Douglas C. Michael, *Federal Agency Use of Audited Self-Regulation as a Regulatory Technique*, 47 Admin. L. Rev. 171, 182 (1995).

[46] See Saule T. Omarova, *Wall Street as a Community of Fate: Toward Financial Industry Self-Regulation* 159 U. Pa. L. Rev. 411 (2011) for a discussion of this issue.

[47] See *Id.*

noted above, there are only 104 nuclear power plants in the U.S.,[48] and only 98,000 people are employed in the industry,[49] compared with over 800,000 in the financial industry[50]. And due to the regulatory structure of the power generation industry, nuclear power plants rarely compete with each other. Furthermore, the technology used in different nuclear power plants is very similar. All these factors helped audited self-regulation to be successful in the nuclear industry.

The financial industry is both larger and less organized than the electrical and nuclear industries, and has seen less success in audited self-regulation Saule Omorova notes that "today's financial industry is expansive, highly diverse, and heterogeneous," as well as "increasingly bifurcated in terms of the size of financial institutions."[51] Different sub-industries in finance, like insurance, retail banking, and investment banking, lead to more heterogeneity and less unity.[52] The world of finance is interconnected, especially with the recent rise of financial products like derivatives which "create unprecedented interconnectedness among financial institutions."[53] But overall, the industry seems to lack a "community of fate" mentality that limits the ability of industry to self-regulate.[54]

In some industries, regulatory safety standards may serve to keep small, new entrants out of the industry. This benefits governments, whose primary interest is promoting safety. It also benefits the large companies that dominate some industries. This is the case the chemical industry, where large chemical companies are better able to comply with safety regulations. In these cases, the private sector incentives for regulation are aligned with the government's interest in regulation, although the risk of suppressing competition arises. Thus, audited self-regulation is more likely to be successful.

Effectiveness of the auditing agency

For audited self-regulation to be effective, the auditing agency must be able to audit effectively. Two problems can get in the way: a lack of technical expertise, and capture of the auditing agency by the regulated industry.

The auditing government agency must also have at least enough technical knowledge to be able to tell whether standards are being met, and whether standards are sufficiently high. As one author put it, "[S]elf-regulation requires the 'auditors' to have technical knowledge sufficient to evaluate compliance, as well as a knowledge of how to test compliance itself."[55]

Furthermore, the auditing agency must avoid being "captured" by the industry. The phenomenon of regulatory capture is well established. Capture involves either regulators who are "purposefully instrumental to the interests of regulated communities to the end of lining their own pockets," or, less heinously, "subject to myriad pressures and incentives that push

---

48 http://www.nei.org/resourcesandstats/nuclear_statistics/usnuclearpowerplants/

49 [Cite]

50 http://selectusa.commerce.gov/industry-snapshots/financial-services-industry-united-states

51 *Id.* at 456.

52 *Id.* at 457.

53 *Id.* at 458.

54 *Id.* at 471.

55 Michael at 195.

regulatory choices in the direction desired by regulated industry."[56] The same danger is present in the world of audited self-regulation, perhaps even to a greater extent. Audited self-regulation features a governmental auditing agency working in cooperation with a non-governmental, standard-setting agency (the SRO). A close relationship between the SRO and the auditing agency could result in a loss of independence for the auditing agency and lead to ineffective audits.

Closely related, an effective self-regulatory organization is just as important for a program of audited self-regulation. Like an auditing agency, a SRO can be ineffective because of lack of technical knowledge or capture by industry. In most cases an SRO will do the majority of the technical work and the set standards, so expertise on the part of the SRO is critical.

The financial industry offers one example of the problems of industry capture. Although the auditing agency (the SEC) is thought to be independent, the self-regulatory organization (FINRA) may have been "captured" by industry to some extent. The recent scandal involving Bernie Madoff suggests that this may be the case. Madoff was on the board of the NASD from 1984 until 1987, and held a variety of other positions with NASD and NASDAQ.[57] Bernie Madoff's broker-dealer was registered with FINRA/NASD since 1960. One commentator asked why FINRA didn't catch Madoff earlier, and noted that "idealistic public-spirited types are not likely to seek careers as FINRA examiners," but rather, work for the SEC, and "those examiners who do yearn for a better life in financial services are not likely to want to rankle future employers by performing an examination with too much diligence."[58] He ultimately concluded that "the industry is not truly a participant in its own regulation, except as a lobbyist for business friendly, and often anti-competitive rule-making."[59] By contrast, regulatory agencies in the nuclear energy have avoided capture and have been much more successful. As mentioned above, INPO's success was due partly to the fact that the organization made credible threats to reveal non-compliance with programs to the Nuclear Regulatory Commission. The independence of the regulatory agency was essential.

AUDITED SELF-REGULATION IN THE PROPOSED CYBERSECURITY ACT

The first task of the Department of Homeland Security ("DHS") under the Cybersecurity Act of 2012 would be to begin the process of sector by sector risk assessments and then designated "covered critical infrastructure." The broad definition of what might be "covered critical infrastructure" leaves open the question of how much DHS may designate as covered.

The Act adopts the USA PATRIOT Act's definition of "critical infrastructure:"

> systems and assets, whether physical or virtual, so vital to the United States that

---

56 Matthew D. Zinn, *Policing Environmental Regulatory Enforcement: Cooperation, Capture, and Citizen Suits*, 21 Stan. Envtl. L.J. 81, 108 (2002).

57 http://www.finra.org/Newsroom/Speeches/Luparello/P117765

58 http://www.tradersmagazine.com/news/102896-1.html?pg=2

59 *Id.*

the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" P.L. 107-56 sec. 1016(e).

The USA PATRIOT Act definition of critical infrastructure has been used to designate a broad range of sectors as critical, including: Agriculture, Food, Water, Public Health, Emergency Services, Government, Defense Industrial Base, Information and Telecommunications, Energy, Transportation, Banking and Finance, Chemical Industry, and Postal and Shipping.[60]

However, the coverage of the Cybersecurity Act of 2012 is not quite as broad as the coverage of the USA PATRIOT Act. Although the Cybersecurity Act adopts the USA PATRIOT Act's definition of what "critical infrastructure" is, it only allows DHS to designate a subset of critical infrastructure as "covered critical infrastructure, " including any

> "system or asset . . . if damage or unauthorized access to that system or asset could reasonably result in -
>
> (i) the interruption of life-sustaining services, including energy, water, transportation, emergency services, or food, sufficient to cause –
>
> (aa) a mass casualty event comparable to the consequences of a weapon of mass destruction; or
>
> (bb) mass evacuations of a major population center or a large geographic area in the United States;
>
> (ii) catastrophic economic damage to the United States including:
>
> (aa) failure or substantial disruption of a United States financial market;
>
> (bb) incapacitation or sustained disruption of a financial system; or
>
> (cc) other systemic, long-term damage to the United States economy.
>
> (iii) severe degradation of national security or national security capabilities, including intelligence and defense functions."[61]

During Senate Hearings on this bill, several of the bill's drafters and expert supporters shed light on the type of sectors that they envisioned being covered by this layered definition. Senator Lieberman, the chief sponsor of this bill, began his testimony by describing the sort of dangers that led him to draft this legislation, speaking of the threat that cyber terrorists could "seize control of a city's electric grid or water supply system with the touch of a key from a world away.[62]"

At the same Hearing, Senator Collins echoed similar concerns for the safety of systems "like the power grid, water treatment plants, and key financial systems."[63] Senator John D.

---

60 http://www.fas.org/sgp/crs/RL32631.pdf

61 Cybersecurity Act of 2012, Section 103, p. 14-15.

62 Senator Joseph I. Lieberman. Testimony before Homeland Security and Governmental Affairs Committee, p. 1 February 16, 2012, *available at* http://www.hsgac.senate.gov/hearings/securing-americas-future-the-cybersecurity-act-of-2012

63 Senator Susan M. Collins, Testimony before Homeland Security and Governmental Affairs Committee, p. 1 February 16, 2012.

Rockefeller painted the mass casualty potential of cyber interruption of transportation systems such as the "air traffic control system" or rail road "rail switching networks."[64] Senator Feinstein's testimony mentioned the critical importance of computer networks, credit card & bank ATM systems.[65] Although this combined testimony suggests a consensus over potential covered critical infrastructure--the electric grid, water and sewage systems, transportation, some financial sectors--other testimony called into question how much the bill would actually cover. Hon. Stewart A. Baker testified that the definition in the bill may make it too easy to avoid a designation as covered, saying that according to the definition in the bill, "an individual infrastructure owner, such as a rural electricity provider, has no responsibility under this title if it can show that an undefended cyberattack would only cause an *ordinary* number of fatalities?" The text of the Cybersecurity Act of 2012 requires the potential for "mass casualties," "catastrophic" impact, or "severe degradation" before DHS designates a system as "covered." Baker emphasizes that the bill would allow individual owners of infrastructure covered as critical to challenge that designation successfully in court with an argument that their failure to protect against cyber attack would only have the potential to kill a few people.[66] In sum, the Cybersecurity Act of 2012 grants coverage that is unlimited in what sectors it may be encompassed, but very stringent in the degree of risk that must be posed before DHS acts.

The remainder of this section examines several sectors that are likely to be designated as "covered critical infrastructure" under the proposed Act and uses the factors sketched earlier to analyze the likely efficacy of this Act's audited self-regulation structure as a regulatory tool in each of those sectors. In the electrical and nuclear industries, for instance, audited self-regulation is likely to be successful under the Act as it has been previously. Most firms in those sectors recognize the inevitability of regulation, and they recognize that no one firm benefits if a disaster befalls another. Moreover, past practice suggests that both the auditing agency and relevant SROs have not been captured by industry. The potential impact in other sectors is not as clear.

Chemical

Pursuant to the DHS Appropriations Act, 2007, H.R. 5441, the Secretary of the DHS has already been issuing rules and policies relating to the security of the chemical industry.[67] This is because the chemical industry was considered to be one of seventeen critical infrastructures capable of causing

---

64 Hon. John D. Rockefeller IV, Testimony before Homeland Security and Governmental Affairs Committee, p. 3 February 16, 2012.

65 Hon. Dianne Feinstein, Testimony before Homeland Security and Governmental Affairs Committee, p. 1-2 February 16, 2012.

66 Hon. Stewart A. Baker, Testimony before Homeland Security and Governmental Affairs Committee, p. 6 February 16, 2012.

67 DHS Appropriations Act, 2007, H.R. 5441, "This bill authorizes spending for the construction of hundreds of miles of fence along the Mexico-US border, and increased nuclear-detection equipment in ports. Regarding chemical plant security, it authorizes the DHS to check security at chemical plants. The DHS must issue "risk-based performance standards" for chemical plants within six months."

"catastrophic" damage.[68] This is a reasonable conclusion given that many of the ingredients for manufacturing weapons of mass destruction are chemical. Moreover, accidents at chemical facilities are capable of causing mass casualty or mass evacuation of population centers. Because the Cyber Security Act will likely be implemented in a similar manner as the current DHS implementation, the chemical industry is a good place to start our analysis of the likely success of the self regulation strategy.

The chemical industry appears to be a good candidate for audited self regulation because most of the determinants that we have identified exist in this industry. The industry recognizes the inevitability of regulation due to the well publicized failures in the past. The industry is very sensitive to the possibilities of government over-regulation. Similar to what the Chernobyl accident did for nuclear power industry, the Bhopal accident in 1989 caused great panic among the public and government agencies regarding safety standards in the chemical industry. Many believe the Responsible Care Program was started by the ACC as a way to avoid stricter government regulations in the wake of the Bhopal accident.[69] It is not hard to believe the industry also recognizes the potential for a similar public backlash if a terrorist attack is successfully carried out through a chemical facility.

The regulations and rules needed to prevent a catastrophic terrorist attack require persons with specialized knowledge in both design and implementation. Knowledge is required for what types of chemicals are potentially dangerous as well as how they may be deployed by potential terrorists. The list of chemicals of interest developed by the DHS was a result of combining similar lists from other regulations, such as OSHA, and comments from industry insiders.[70] Additionally DHS stresses the performance standards approach, leaving the specific measures to achieve the outcome up to the discretion of the regulated entity.[71] Although the DHS publishes a list of potential procedures for the facility owner to choose from, the procedures are meant to be illustrative rather than a closed universe of options. A facility is free to adopt and implement any security measures or practices appropriate to its circumstances, so long as DHS determines that those measures are adequate to meet the applicable risk based performance standard.[72] It is easy to see why this type of flexible approach would be preferable to individual members of the chemical sector as opposed to a strict one size fits all regulatory approach. Thus the incentive to adhere to the regulations and thus keeping the current flexible approach is high.

The industry already has a self organized trade association called the American Chemistry Council ("ACC"), which has been in existence since 1872.[73] The ACC includes 180 firms that produce the majority of chemicals in the United States by volume.[74] Furthermore, the members of the industry are frequently engaged in the buying and selling of their products amongst themselves, adding another incentive for the industry to self-organize. The extensive amount of cooperation within the industry, along with the long history of self-organization, provides incentives to the individual members to align their interests with those of the industry. Any member that steps out of line will likely be ostracized by its peers in addition to receiving penalties from the regulatory agencies.

---

68 http://www.fas.org/sgp/crs/RL32631.pdf

69 Without Sanctions

70 6 CFR Part 27, Appendix to Chemical Facility Anti-Terrorism Standards; Final Rule.

71 Risk-Based Performance Standards Guidance, Chemical Facility Anti-Terrorism Standards, May 2009.

72 Id.

73 Industry Self-Regulation without Sanctions: The Chemical Industry's Responsible Care Program,"Without Sanctions", The Academy of Management Journal, Vol. 43, No. 4 (Aug., 2000), pp. 698-716.

74 Without Sanctions

Compared to the Responsible Care Program, an unsuccessful voluntary self regulation program started by the ACC, the DHS program will provide the explicit sanctions in its implementation lacking in the Responsible Care Program.[75] The program under DHS provides for civil liabilities of up to 25,000$ per day for violating an order, and injunctions for more serious violations.[76] This likely will provide the floor of acceptable behavior that eliminates the dangers of a competitive race to the bottom at the expense of the public interest.[77]

In conclusion, because the chemical industry recognizes the inevitability of government regulation and prefers flexible regulation, audited self regulation is plausible. Moreover, in light of the fact that the interests of the private sector and government are aligned, the audited self-regulation scheme will likely be successful here. The addition of specific penalties for those that fail government audits will likely be the difference in success in contrast to the past shortcomings of voluntary self-regulations by the industry in the past.

Internet Communication

Our daily lives are so intertwined with the internet that it is difficult to imagine living without it. Certainly a breakdown of internet service may cause an "interruption of life-sustaining services" or "catastrophic economic damage" through a breakdown in communication and data storage services that is the backbone of business operations. Moreover, the internet may be covered under two of the seventeen critical infrastructures, information technology and communications, defined by the Department of Homeland Security pursuant to President George Bush's presidential decision directive 63.[78] The information technology sector includes hardware, software, and IT systems and services, and – in collaboration with the communications sector – the Internet.[79] The communications sector includes providers of terrestrial, satellite, wireless, and wire-lines for communication.[80] The communication sector provides the critical control systems, services, and physical architecture (including the internet infrastructure).[81]

Although it would be reasonable to conclude that the internet would be covered under the proposed Cybersecurity Act, it is unclear whether this would in fact be true. Under the Act, the Secretary may not designate as covered critical infrastructure "an information technology product or service based solely on finding that the product or service is capable of, or is actually, being used in covered critical infrastructure; [or] a commercial information technology product, including hardware and software."[82] The term commercial information technology product is very broad under the Act, it means any

---

75 The Role of Private Decentralized Institutions in Sustaining Industry Self-Regulation. Organization Science, Dec., 2006, 677.

76 6 C.F.R. §27.300

77 Conscience of a Progressive,Ernest Partridge,Chapter Seventeen:Corporate Self-Regulation: A Case History.

78 Department of Homeland Security, Critical Infrastructure Sectors (2009), available at http://www.dhs.gov/files/programs/gc_1189168948944.shtm.

79 Department of Homeland Security, National Infrastructure Protection Plan, Information Technology Sector, (2009) available at *http://www.dhs.gov/xlibrary/assets/nipp_snapshot_informationtechno*logy.pdf.

80 Department of Homeland Security, National Infrastructure Protection Plan, Communications Sector (2009) available at *http://www.dhs.gov/xlibrary/assets/nipp_snapshot_communications.pdf*.

81 Department of Homeland Security, National Infrastructure Protection Plan, Communications Sector (2009) available at *http://www.dhs.gov/xlibrary/assets/nipp_snapshot_communications.pdf*.

82 Cybersecurity Act of 2012, Section 103, p. 15-16

"commercial item that organizes or communicates information electronically."[83] The term commercial item means "an item, other than real property, that is of a type customarily used by the general public or by nongovernmental entities for purposes other than governmental purposes; and has been sold, leased, or licensed, or offered for sale, lease, or license, to the general public."[84]

On its face, the exception covers any component, from home computers and cell phones to satellites or fiber optic lines, which uses or carries electronic information. To give the term such a broad meaning would vitiate the Act's purpose, since the majority of actions taken by a facility owner would presumably be related to electronic information. The tension that exists between the purpose of the Act and the information technology exception contained in it highlights one of the difficulties confronted by the proponents of this bill. There needs to be a balancing between the need for increased cyber security with the need for continued growth of American businesses that are based on the internet.

Even if the Act applies to the internet, the business realities of the sector suggest that the audited self-regulation scheme would not be successful. Although internet providers fear government overreaching, they have thus far avoided almost all forms of government regulation. There are no industry-specific regulations that govern backbone provider dealings, instead they use "peering" and "transit" agreements amongst themselves, governed only by laws of contract and property.[85] Furthermore, there have been no disasters such as Chernobyl or Enron to lower the industry's reputation in the eyes of the public. The lack of a publicly recognizable catastrophe gives the service provider industry little reason to fear public outcries for the government to step in.

The lack of a publicly recognizable disaster, along with the relatively short history of the internet, has resulted in an industry that is not very well organized. Unlike the nuclear or chemical industry, the businesses in the internet provider industry are involved in a diverse array of business endeavors. They provide services through vastly different technologies including land-lines, wireless, and satellite communication, often simultaneously. Many members of the industry are also involved with content delivery through the internet, while others are also involved with hardware manufacturing. Because the participants lack closely aligned goals and practices, it is nearly impossible for the organization to organize effectively along clearly defined goals.

Moreover, the speed and interconnectedness of the internet creates a free-rider problem when it comes to system security expenditures. Vulnerabilities to attacks often come from a weak link outside the system administrator's control, and the benefit of a local secure network is freely enjoyed by everyone that connects to the network. The complications in pinpointing sources of attack make assigning blame to the proper party difficult, creating an economic externality. This high cost of implementation drives the incentives of the private owners further apart from the regulator, thus making audited self-regulation unlikely to succeed.

Finance

There is no doubt that a disaster in the financial markets can cripple the country. The lack of available capital can bring the economy to a halt. The 2008 recession is testament to the fact that cyber infiltration of the financial sector could be an effective terrorist goal.

---

83 Cybersecurity Act of 2012, Section 2, p. 3.

84 41 USC § 103 (2011)

85 Michale Kende, The Digital Handshake: Connecting Internet Backbones 2, FCC Office of Plans and Policy, Working Paper No. 32, (2000).

The financial sector is one of the largest and most complex sectors in the U.S. economy. In 2011 it provided 8.4% of the nation's gross domestic product.[86] The financial sector is as diverse as it is large: national banks, savings and loan associations, commodities exchanges, securities exchanges, financial advisers, and other sub-industries all face different regulatory schemes. Is the audited self-regulation in the proposed Cybersecurity Act likely to work in finance, based on the factors discussed above?

Government regulation of some kind is inevitable in finance, but the extent of such regulation is not. And in fact, the historical precedent of "bailouts" for troubled financial sector companies may actually create a disincentive for the financial industry to create meaningful self-regulation, as Saule Omorova argues, noting that the sector "currently enjoys extra-ordinary security through its access to an extensive public safety net and the near certainty of government bailouts in the event of a crisis."[87]

On the other hand, the natural interest of financial companies in preventing cybersecurity breaches is well aligned with the government's interest in preventing cybersecurity breaches. Financial companies suffer from security breaches that expose customer information, both from loss of trust in the financial institution and direct monetary damage. The recent security breach at Global Payments Inc., which exposed personal data of hundreds of thousands of credit card customers,[88] exemplifies the type of breach both industry and government would like to prevent.

Any regulation must defer to the expertise of the private firms in the financial world. Current regulations recognize this and delegate significant authority to financial institutions to create plans for securing customer information. As a Federal Reserve web site puts it, "Each financial institution must identify and evaluate risks to its customer information, develop a plan to mitigate the risks, implement the plan, test the plan, and update the plan when necessary."[89] Thus, it makes sense that cybersecurity regulations for the financial sector would delegate significant authority to companies and SROs. It may be difficult for DHS to acquire all the specialized knowledge necessary to regulate each company by itself.

Bringing the financial community together on a common plan, however, is daunting. The financial sector is fragmented and member companies do not have a strong sense of cooperation with the industry. That is the argument of Saule Omorova, who argues that the industry lacks a "community of fate" mentality which could encourage cooperation and effective self-regulation.[90] This argument is highly relevant for traditional financial sector regulations, but may not be as important for the cybersecurity arena. One important private industry agency, the Financial Services Sector Coordinating Council (FSSCC), already works with federal regulators on cybersecurity issues. This suggests that there may be more of a "community of fate" within the financial sector regarding cybersecurity issues than for traditional financial regulations.

Any auditing agency will need to have both the technical capability to audit and avoid capture by the industry. This has been a problem for SROs in the financial sector, like FINRA, in the past. Perhaps in light of those historical shortcomings, the proposed Cybersecurity Act

---

86 http://corpgov.proxyexchange.org/2012/01/financial-sector-at-peak-percent-of-gdp/ (accssed 4/11/2012 4:50 PM).

87 Omorova at 4.

88 http://online.wsj.com/article/SB10001424052702303816504577313411294908868.html (accessed 4/11(2012 4:54 PM).

89 http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm

90 Omorova at 4.

designates DHS as the ultimate auditing authority for cybersecurity issues. Presumably, DHS has less of a connection with the financial sector, which could help mitigate the capture issue.

Although the question is close, we are skeptical that audited self regulation will work well in the financial sector. The sector is too fragmented and no consensus is likely to emerge as to the inevitability of cyber regulation in the field. Moreover, given that even leading financial firms at times seem to lack a basic understanding of their trades and proprietary systems, it seems a stretch to think that DHS will develop the wherewithal to audit effectively.

CONCLUSION

Audited self-regulation is a useful, if limited, tool for government. As noted above, certain factors like the homogeneity of the sector and the fear of government takeover bear on whether a program of audited self-regulation is likely to be successful. The Cybersecurity Act of 2012 is likely to have mixed results: it is more likely to be successful in the chemical industry, and less so in the financial industry.

With this in mind, Congress could make certain modifications to the Act. One proposal would be to enact the Act as is, monitor the results, and make changes as necessary in one or two years. This would allow for flexibility with more difficult to regulate sectors such as finance. Another option would be to grant the Department of Homeland Security the authority to use different regulatory methods in different fields. For example, the nuclear industry could be governed by audited self-regulation, while the financial sector could be governed by command and control regulation. But the disadvantage of this approach is that it would afford an opportunity for interest groups to lobby for preferred types of regulation. Another option would be to use a system of modified command and control regulation that provided companies with incentives for compliance: e.g., holding companies responsible for two times the monetary damages caused by a cyberattack. In sum, audited self regulation in the proposed Act represents a sound course, but not for every critical infrastructure affected.