Executive Order 13636: Improving Critical Infrastructure Cybersecurity

Incentives Study Analytic Report

Publication: June 2013
Department of Homeland Security Integrated Task Force

Table of Contents

1. BACKGROUND

In February 2013, the President signed Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," and Presidential Policy Directive (PPD)-21, "Critical Infrastructure Security and Resilience."[1] [2] That same day, President Obama warned in his State of the Union Address:

> America must also face the rapidly growing threat from cyber-attacks. We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.

The policies set forth in these directives are intended to strengthen the security and resilience of critical infrastructure against evolving threats and hazards, while incorporating strong privacy and civil liberties protections into every cybersecurity initiative. These documents call for an updated and overarching national Framework that reflects the increasing role of cybersecurity in securing physical assets.

Securing critical infrastructure against growing and evolving cyber threats requires a layered approach. The Department of Homeland Security (DHS) actively collaborates with public and private sector partners every day to prevent, protect from, respond to, and coordinate mitigation efforts against attempted disruptions and adverse impacts to the nation's critical cyber and communications networks and infrastructure, as well as a range of additional hazards, including terrorism and natural disasters.

DHS is the Federal Government's lead agency for coordinating the protection, prevention, mitigation, and recovery from cyber incidents. DHS also works regularly with business owners and operators to strengthen their facilities and communities by sharing cyber and other threat information.

1.1. DHS Integrated Task Force and Incentives Working Group

To implement EO 13636 and PPD-21, DHS established an Integrated Task Force (ITF) to lead DHS implementation, coordinate interagency and public and private sector efforts, and ensure effective integration and synchronization of implementation across the homeland security enterprise.

The ITF is currently comprised of eight Working Groups each focused on specific deliverables of implementation. Among these eight Working Groups, the Incentives Working Group was established to lead the study of incentives for participating in the voluntary critical infrastructure cybersecurity program.

1.2. Incentives Study Requirements

EO 13636 and PPD-21 are intended to strengthen the security and resilience of critical infrastructure through an updated and overarching national Framework that acknowledges the increased role of cybersecurity in securing physical assets. The government and the private sector have a mutually shared interest in ensuring the viability of critical infrastructure, and the provision of essential services, under all conditions. Critical infrastructure owners and operators are often the greatest beneficiary of investing in their own security, and they have a social responsibility to adopt best practices for cybersecurity. However, the private sector may be justifiably concerned about the return on security investments that may not yield immediately measurable benefits. Effective incentives can help the private sector justify the costs of improved cybersecurity by balancing the short-term costs of additional investment with similarly near-term benefits.

[1] http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
[2] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Section 8(d) of EO 13636 includes the following requirement:

> (d) The Secretary [of Homeland Security] shall coordinate establishment of a set of incentives designed to promote participation in the [voluntary cybersecurity] Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

The U.S. Intelligence Community's March 2013 Worldwide Threat Assessment describes increasing risk to U.S. critical infrastructure from cyber attacks, as well as eroding U.S. economic and national security from cyber espionage.[3] Addressing these risks is a top priority for the Federal Government in its responsibility for ensuring the safety and security of the Nation. However, the owners and operators of critical infrastructure often have more immediate business priorities, as well as information gaps, which hinder the adoption of higher levels of cybersecurity.

While some market-based incentives exist to improve the cybersecurity of critical infrastructure, independent of government intervention, the pace of the necessary improvement in cybersecurity needs to be hastened in order to more rapidly counter the increasing risk of cyber attacks and cyber espionage. As such, it is appropriate to consider where government action can provide additional impetus to the market, while acknowledging that there are places where market-based incentives may perform adequately independent of government intervention.[4] The three independent incentives studies required by EO 13636 seek to make recommendations to accelerate the current levels of cybersecurity by making recommendations to support and expand existing market incentives. Though each of the incentives considered in this study acts by influencing the market for cybersecurity-related products and services, each requires some degree of government intervention to meet the aims of EO 13636.

2. ANALYSIS

Given the requirements in EO 13636, the ITF Incentives Study had three objectives:

1. Recommend a set of incentives designed to promote adoption of the Cybersecurity Framework under development by the National Institute of Standards and Technology (NIST).
2. Evaluate the benefits and relative effectiveness of each of these incentives in promoting adoption of the Framework under development by NIST.
3. Determine which of these incentives require legislation and which can be provided under existing law and authorities.

For the purpose of this study, DHS used the following definition of incentive: ***a cost or benefit that motivates a decision or action by critical infrastructure asset owners and operators to adopt the Cybersecurity Framework under development by NIST***. For example, this can include grants, insurance, liability considerations, procurement preferences or requirements, public recognition, subsidies, and tax incentives, to name a few.

The scope of the study included the possible incentives that the Federal Government could use—either under existing law and authorities or only through new legislation—to encourage the investment required for adoption of

[3] Accessed at: www.intelligence.senate.gov/130312/clapper.pdf
[4] Certain industries have already implemented voluntary and mandatory approaches and standards to cyber protection, including bulk electricity transmission through FERC regulations.

the voluntary Cybersecurity Framework by the owners and operators of critical infrastructure assets within the 16 critical infrastructure sectors defined under PPD-21.

Overall, the study methodology included the following, described in the pages that follow:

1. Review of known cybersecurity incentive proposals
2. Verification of the initial list of incentives
3. Development of the microeconomic model
4. Research
5. Finalization of the list of incentives
6. Application of the microeconomic model

In addition, an initial review of legal feasibility and policy implementation considerations related to incentive adoption was conducted and is described separately along with the DHS recommendations in the DHS Incentives Study report.

2.1. Review of Known Cybersecurity Incentive Proposals

DHS began by conducting an initial review of known cybersecurity incentive proposals to define the range of incentives to be included in the study and to confirm the requirements those incentives were intended to meet. This review included proposals made by academic, advocacy, Federal, and private sector stakeholders. It included a literature review of publicly available proposals, as well as interviews and Working Group meetings with stakeholders. The review yielded the following known government and industry sources of cybersecurity incentive proposals:

1. Cybersecurity Act of 2012, February 14, 2012 [5]
2. DHS Blueprint for a Secure Cyber Future, November 2011 [6]
3. Recommendations of the House Republican Cybersecurity Task Force, October 2011 [7]
4. Department of Commerce, Internet Policy Task Force, *Cybersecurity, Innovation, and the Internet Economy* (Green Paper), June 2011 [8]
5. Business Software Alliance, the Center for Democracy and Technology, the Internet Security Alliance, TechAmerica, and the U.S. Chamber of Commerce, *Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper*, March 8, 2011 [9]
6. Cross Sector Cybersecurity Working Group (CSCSWG), Incentives Subgroup, *Incentives Recommendations Report*. September 2009. [10]
7. President's Cyberspace Policy Review, May/June 2009 [11]
8. Internet Security Alliance, *Issue Area 3: Norms of Behavior—Hathaway Questions*, March 24, 2009 [12]

Collectively, these sources contained a set of 14 broad categories of both remunerative and coercive incentives, which served as an initial focus of inquiry. The list below was simply intended to represent the initial descriptive

[5] Accessed at: http://www.hsgac.senate.gov/download/the-cybersecurity-act-of-2012-s-2105
[6] Accessed at: http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf
[7] Accessed at: http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf
[8] Accessed at: http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf
[9] Accessed at: http://www.bsa.org/~/media/Files/Policy/Security/CyberSecure/cybersecurity_white_paper_publicprivatepartnership.ashx
[10] Obtained from White House National Security Staff
[11] Accessed at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[12] Accessed at: http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20ISSUE%20AREA%203%20-%20NORMS%20OF%20BEHAVIOR--HATHAWAY%20QUESTIONS.pdf

cataloging of the major incentive categories contained within the eight sources listed above, and does not represent either the recommendations or the economic or legal analyses required by EO 13636.

1. Expedited Security Clearance Process: establish a procedure to expedite the provision of security clearances to appropriate personnel employed by critical infrastructure owners and operators under the Framework.
2. Grants: direct federal funding for investment in cybersecurity products and services that would allow adoption of the Framework; alternatively, condition existing grant programs to adoption of Cybersecurity Framework.
3. Include Cybersecurity in Rate Base: allow rate recovery of cybersecurity investments in the rates charged for services provided by Framework adopters.
4. Information Sharing: implement a procedure for ensuring that Framework adopters are provided with relevant near real-time cyber threat information.
5. Insurance: promote cybersecurity insurance through related incentives and/or federal reinsurance programs to help underwrite the development of cybersecurity insurance programs.
6. Liability Considerations: capped liability in exchange for improved cybersecurity or increased liability for the consequences of poor security.
7. New Regulation/Legislation: for example, a combination of insurance requirements and liability protections for organizations that adopt the Framework.
8. Prioritized Technical Assistance: ensure Framework owners and operators receive prioritized cybersecurity technical assistance
9. Procurement Considerations: offer preferential consideration in the procurement process for Framework owners and operators and/or requiring Framework adoption by federal goods/services providers.
10. Public Recognition: create an award for companies that adopt the Framework and/or best practices; voluntary certification/accreditation for Framework adoption.
11. Security Disclosure: require public notification of disclosures to encourage owners and operators to take care to avoid breaches.
12. Streamline Information Security Regulations: create unified compliance model for similar requirements and eliminate overlaps among existing laws (e.g., Sarbanes-Oxley, the Health Insurance Portability and Accountability Act of 1996, or HIPAA, and Gramm-Leach-Bliley).
13. Subsidies: fund direct purchase of cybersecurity products and services for Framework owners and operators.
14. Tax Incentives: provide tax credits and/or deductions for Framework adopters.

Table 1 below illustrates the distribution of these incentives among the eight sources.

***Table 1.** Distribution of Incentive Categories by Source*

	Incentive Description	CSA 2012	DHS Blueprint 2011	House Republican Task Force 2011	Commerce Green Paper 2011	BSA, CDT, ISA, TA, Chamber of Commerce 2011	CSCSWG 2009	President's CSPR 2009	ISA 2009
1	Expedited Security Clearance Process	X							
2	Grants		X	X		X	X		X
3	Include Cybersecurity in Rate Base								X
4	Information Sharing	X			X				
5	Insurance			X	Y	X	Y		X
6	Liability Considerations	X	X	X	Y	X		X	X
7	New Regulation/Legislation					X	Y	X	X
	(e.g. Cyber SAFETY Act)					X	Y		X
8	Prioritized Technical Assistance	X							
9	Procurement Considerations	X					X	X	X
10	Public Recognition	X					Y		X
11	Security Disclosure				X				
12	Streamline Information Security Regulations			X		X	X		X
13	Subsidies		X				X		X
14	Tax Incentives		X	X		X	X	X	X

Key

X indicates that the incentive was recommended by the source

Y indicates that the incentive was discussed by the source but not formally recommended

2.2. Verification of the Initial List of Incentives

To review, refine, and expand the preceding list of incentives, the list was presented to (1) a meeting of the full ITF on March 8, 2013, (2) the interagency representatives of the ITF Incentives Working Group on March 20, 2013, and (3) interagency and industry stakeholders—including representatives from both the Partnership for Critical Infrastructure Security and the Cross Sector Cybersecurity Working Group—at the Incentives Working Group on March 27, 2013.

At each of these presentations, representatives were asked to review the list and to offer any additional incentive categories, or sub-categories to the existing broadly defined categories, that the Federal Government should consider. Based on feedback received from the March 27, 2013 Working Group meeting, the additions highlighted in bold below were made to six of the 14 incentives.

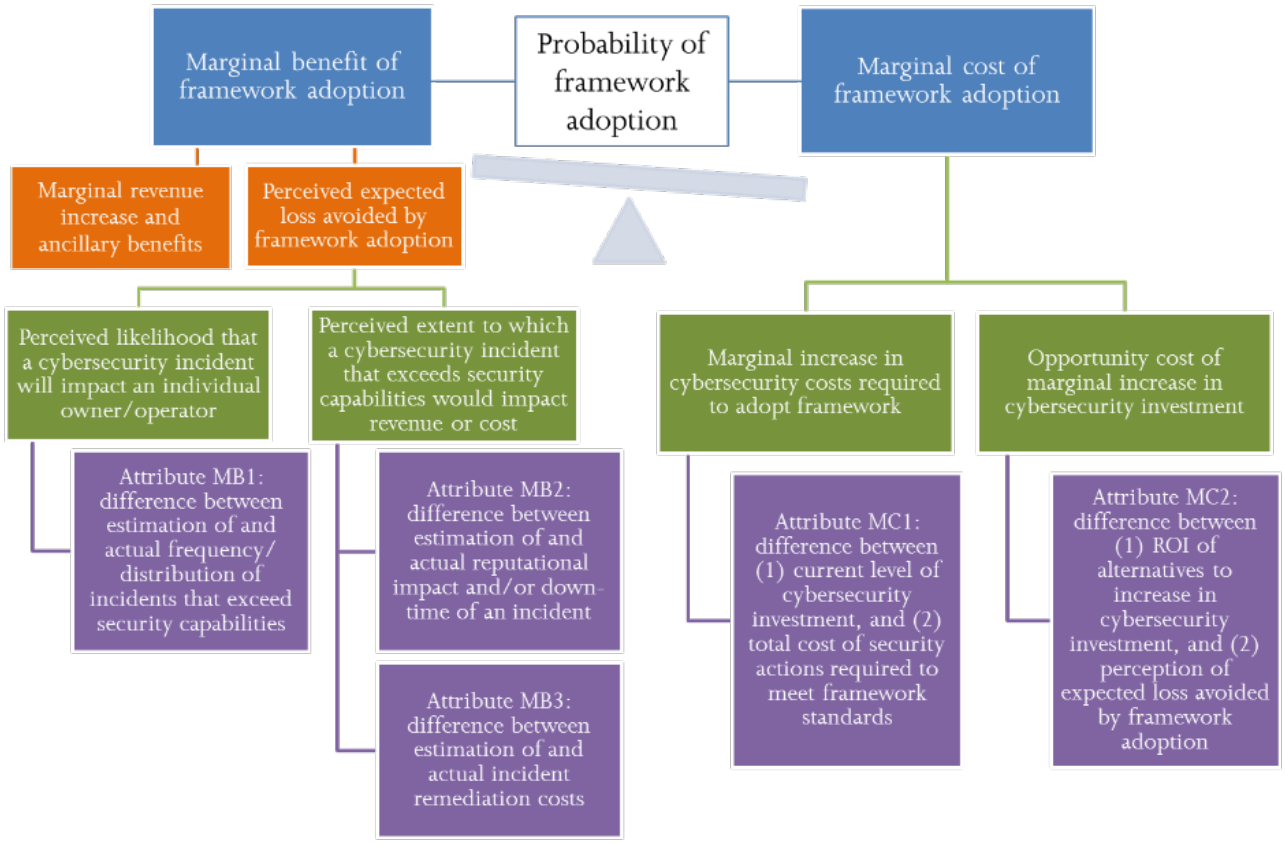
- Expedited Security Clearance Process: expedite the provision of security clearances to appropriate personnel employed by CI owners and operators under the Framework, **as well as expedited Sensitive Compartmented Information Facility (SCIF) sponsorship**.
- Liability Considerations **and Legal Benefits**: reduce liability in exchange for improved cybersecurity or increased liability for the consequences of poor security; **full indemnity, higher burdens of proofs, or limited penalties; case consolidations; case transfers to a single federal court; creation of a federal legal privilege that also preempts State litigation discovery law and applies to owners and operators that undertake cybersecurity self-assessments so that those assessments would not be discoverable in subsequent litigation and/or used as evidence in court**.
- Security Disclosure: require public notification of disclosures to encourage owners and operators to take care to avoid breaches; **preemption of state notice requirements**.
- Streamline Information Security Regulations: create unified compliance model for similar requirements and eliminate overlaps among existing laws (e.g. Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley); **streamline differences between U.S. and international law (perhaps through treaties); allow equivalent adoption (so that companies wouldn't need to adopt the Framework if they're already doing something equivalent); reduce the audit burden; move to the head of the line with prioritized permitting**.
- Subsidies: fund direct purchase of cybersecurity products and services for Framework owners and operators; **low-interest financing options or loans**.
- Tax Incentives: provide tax credits or deductions for Framework owners and operators; **decreased rate on capital gains for investors in companies adopting the Framework**.

2.3. Development of the Microeconomic Model

As noted above, given the requirements set forth in EO 13636, the core analytic objective for this study is to evaluate the benefits and relative effectiveness of each of these incentives in promoting adoption of the voluntary Cybersecurity Framework. While the incentives study is required within 120 days of the date of EO 13636 (June 12, 2013), the preliminary version of the Cybersecurity Framework is required within 240 days of the date of the EO 13636 (October 10, 2013). Therefore, since the set of standards, methodologies, procedures, and processes that will comprise the Cybersecurity Framework are unknown at the time of this writing, the incentives that are intended to promote its adoption must be assessed prospectively, in terms of the likelihood that they will motivate organizations to adopt the Cybersecurity Framework in the future. More specifically, the core analytic question that this study seeks to inform is: to what extent would each of the incentives considered

affect the probability that critical infrastructure asset owners and operators will adopt the Cybersecurity Framework under development by NIST? To answer this question, DHS developed the conceptual microeconomic model in Figure 1.

Figure 1. Microeconomic Model



The conceptual microeconomic model presented in Figure 1 is designed to consider the probability of Framework adoption in terms of its marginal benefit and marginal cost for each prospective organization. Marginal cost-benefit analysis is appropriate because it assesses only the changes in benefits and costs associated with Framework adoption, rather than the full benefits and costs associated with all of the cybersecurity standards, methodologies, procedures, and processes within the Framework irrespective of whether some have already been adopted. For example, some prospective adopters may have adopted very few, if any, of the cybersecurity standards, methodologies, procedures, and processes that will be in the Framework. Others with high levels of technological sophistication may have adopted cybersecurity standards, methodologies, procedures, and processes that exceed the Framework in all respects. In each case, the probability of Framework adoption will be a function of the marginal benefit of only those cybersecurity standards, methodologies, procedures, and processes that prospective organizations would apply as they adopt the Framework.

More specifically, the marginal benefit of Framework adoption is composed of (1) marginal revenue increase and ancillary benefits, and (2) the perceived expected loss avoided by Framework adoption. Marginal revenue increases could be associated with tangible financial gains such as Federal procurement or public recognition incentives. Ancillary benefits could be associated with incentives that lower business expenses, such as streamlining existing information security regulations by providing reductions in non-Framework adoption costs (e.g. consolidating audit requirements).

Another set of benefits is related to the perceived expected loss, or perceived risk, avoided by Framework adoption. This is, in turn, composed of two elements:

1. The perceived likelihood that a cybersecurity incident will impact an individual owner or operator. This perceived likelihood is presumably lowered by Framework adoption. This is defined by attribute MB1, the difference between estimation of and actual frequency and distribution of incidents that exceed security capabilities.

2. The perceived extent to which a cybersecurity incident that exceeds security capabilities would impact revenue or cost. This is defined by attribute MB2, the difference between estimation of and actual reputational impact and/or down-time of an incident, and attribute MB3, the difference between estimation of and actual incident remediation costs.

Risk avoidance is qualified as *perceived* expected loss avoidance because information about the likelihood and impact of cybersecurity incidents is interpreted and characterized by individuals and organizations in ways that are not simply based on fact, but is also related to the degree to which it the risk is observable or known and uncontrollable or dreaded.[13] The growing field of behavioral economics, rooted in the work of Kahneman and Tversky, has much to offer on the importance of considering perceived loss.[14] Incentives that increase the perceived expected loss avoided by Framework adoption include Bundled Insurance Requirements, Liability Protections, and Legal Benefits; Prioritized Technical Assistance; and Security Disclosure. These all can be categorized as benefits as they lower the perceived losses related to cybersecurity incidents and, therefore, enhance a business' bottom line.

On the other side of the microeconomic model is the marginal cost of Framework adoption. The marginal cost increase of Framework adoption is composed of two elements. The first is the marginal increase in cybersecurity costs required to adopt the Framework, defined by attribute MC1, the difference between the current level of cybersecurity investment and the total cost of security actions required to meet Framework standards. The second is the opportunity cost of the marginal increase in cybersecurity investment, defined by attribute MC2, the difference between the return on investment of alternatives to an increase in cybersecurity investment and the perception of expected loss avoided by Framework adoption. The incentives that minimize the marginal increase in cybersecurity costs required to adopt the Framework through cost sharing include grants, rate-recovery for price-regulated industries, subsidies, and tax incentives. These have the potential to make it more cost effective for owners and operators to adopt the Framework.

To assess the probability of Framework adoption for each incentive in absolute rather than relative terms, quantitative estimates for each of the elements within each attribute would be required for each prospective organization in order to compare the marginal benefit to the marginal cost for each incentive. These estimates could then be aggregated across all prospective organizations to inform an overall assessment of the absolute probability of Framework adoption for each incentive. Unfortunately, this is not possible due to incomplete and imperfect data. The attributes that define the marginal benefit of Framework adoption are uncertain. Many of the elements within each attribute are currently unknown and many, to some extent, are unknowable. As noted by the National Science and Technology Council's Subcommittee on Networking and Information Technology Research and Development (NITRD), "Secure practices must be incentivized if cybersecurity is to become ubiquitous… The projected benefits must be quantified to demonstrate that they outweigh the costs incurred by

[13] See, for example, Slovic, Fischhoff, and Lichtenstein, "Why Study Risk Perception?" Risk Analysis, Vol. 2, No. 2. 1982.
[14] Kahneman and Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica*, Vol. 47, No. 2. (Mar., 1979), pp. 263-292.

the implementation of improved cybersecurity measures."[15] For these reasons, to apply the microeconomic model described above, evidence was gathered through systematic research to consider the relative effectiveness of each of the incentives through empirical evaluation of relevant voluntary non-cybersecurity incentives.

2.4. Research

Until better data become available, it is not yet possible to quantify the benefits of the Cybersecurity Framework. And until the Framework has been developed, it is similarly not yet possible to estimate the costs of implementing the Framework. Moreover, there are no empirical evaluations of the effectiveness of incentives in promoting the adoption of the Framework, because the Framework is still under development, and the incentives intended to promote its eventual adoption do not yet exist. As a result, the methodology for analyzing the effectiveness of the incentives under evaluation for EO 13636 relies on secondary research of evaluations of voluntary non-cybersecurity programs and largely qualitative methods to assess the relative effectiveness of the incentives. To complement the literature review, stakeholder interviews and workshops were conducted, and responses to the Department of Commerce Notice of Inquiry were reviewed.

2.4.1. Literature Review

Empirical evaluations of voluntary government incentive programs in the literature were considered the primary sources of the secondary research. Since a government incentive program for the adoption of a voluntary Cybersecurity Framework does not yet exist, the literature obviously does not yet include research or evaluations of voluntary cybersecurity incentive programs. One exception is the growing body of research on cybersecurity insurance as an incentive for the promotion of cybersecurity in general, independent of a voluntary Cybersecurity Framework. DHS has recently contributed to the work examining obstacles that hinder the development of the cybersecurity insurance market, having hosted an all-day workshop on cybersecurity insurance in October 2012.[16] Based on stakeholder input during that workshop, DHS held a cybersecurity insurance roundtable in May 2013 that focused on how organizations should build more effective cyber risk cultures. DHS plans to continue this dialogue with stakeholders going forward as the continued development of the cybersecurity insurance market could have significant benefits for future cybersecurity efforts.

For the remaining incentive categories, there exists literature that contains evaluations of those incentives applied to investment in non-cybersecurity voluntary programs that is informative for the analysis and recommendations required by EO 13636. For example, while there are no current tax incentives for cybersecurity investment, there is an extensive literature on the use of tax credits for increasing expenditures on research and development, as well as the effects of tax incentives on tangible, depreciable investments, especially those in equipment. There is also an extensive literature evaluating the use of rate recovery in the form of price cap regulation for electric distribution and transmission networks and telecommunications. Such evaluations of incentives for investment in non-cybersecurity voluntary programs are assumed to be relevant to the study of cybersecurity voluntary programs, though identical results are not assumed.

To scope this effort, the literature review was limited to studies examining relevant incentives. Relevant studies assessed incentives to promote participation in voluntary government programs, and focused upon voluntary investment decisions made by organizations (e.g. rather than individuals or households), wherever available. Studies and research were assessed for quality to inform conclusions about differences among evaluations within incentive categories. For example, articles published in peer-reviewed journals received a high assessment

[15] National Science and Technology Council's Subcommittee on Networking and Information Technology Research and Development, "Trustworthy Cyberspace: Strategic Plan for the federal Cybersecurity Research and Development Program," accessed at http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf
[16] See http://www.dhs.gov/publication/cybersecurity-insurance

of quality, while anecdotal evidence that is not necessarily representative or generalizable received a low assessment of quality.

Interviews with stakeholders, Working Group meetings and Workshops with industry representatives, and responses to the Commerce Notice of Inquiry were used to complement the findings from the literature review, and to help inform conclusions about differences among evaluations as well as about evaluations that are inconclusive.

The literature review was completed with research support from the White House Council of Economic Advisers, the Department of the Treasury's Tax Policy and Federal Insurance Offices, and the Homeland Security Studies and Analysis Institute. The resulting reviews of 144 peer-reviewed journal articles, law review articles, conference papers, working papers, government reports, dissertations, and book chapters are reviewed in Appendix 3.1, and the references are listed in Appendix 3.2.

2.4.2. DHS Incentives Workshop

To complement this research, on Friday, April 19, 2013, DHS hosted an Incentives Workshop. The all-day workshop included two keynote addresses and four panel sessions with time allotted for audience questions and discussion. Approximately 80 interagency and industry participants attended. This section offers a brief summary of the Workshop, and a more detailed summary is included in Appendix 3.3. Workshop participants focused on the following questions:

- How likely is your sector or firm to adopt the voluntary Framework in the absence of new incentives?
- What kinds of incentives are most likely and least likely to promote adoption of the voluntary Framework and why?
- What examples of incentives have worked well for your sector or firm, what types have not worked well, and why?
- Can you think of additional incentive categories the Federal Government should consider?
- What are the likely impacts of the incentives under consideration on your sector or firm?
- What barriers prevent you from taking steps to better address cybersecurity?

The workshop began with keynote addresses from Bruce McConnell, DHS's Acting Deputy Undersecretary for Cybersecurity, and Larry Clinton, President and CEO of the Internet Security Alliance.

Bruce McConnell began by noting that America's national security and economic prosperity are increasingly dependent upon the cybersecurity of critical infrastructure. Because the vast majority of U.S. critical infrastructure is owned and operated by private companies, reducing the risk to these vital systems requires a strong partnership between government and industry. EO 13636 represents an opportunity for the government and the private sector to collaborate in promoting the cybersecurity of the nation's critical infrastructure. Input provided at the Incentives Workshop will represent an essential step toward ensuring that critical infrastructure owners and operators adopt the appropriate security measures to provide essential services to the American people under all conditions.

Larry Clinton outlined the adaptation of other incentives models to cybersecurity, and offered a series of "Incentivization Principles," including that in order to be effective incentives must: be powerful enough to affect corporate investment behavior; be calibrated to match the level of additional investment required to adopt the Framework; vary not just from sector to sector but business to business and thus a menu of incentives will be needed; recognize that regulation that does not include full cost recovery is not a substitute for incentives; and that cost not compensated through incentives will either be passed on to consumers or reduce investment in critical infrastructure.

Session I focused on regulated industries, with panelists from the Federal Energy Regulatory Commission, the American Public Power Association, the National Association of Regulatory Utility Commissioners, the American Gas Association, and the Financial Services sector. Moderated by the President of the Information Technology and Innovation Foundation, panelists discussed a range of issues, including incentives to share information, whether Smart Grid assistance will help utilities with cybersecurity, and rate recovery as an incentive for Framework adoption.

Session II reviewed incentives-related issues specific to non-regulated industries. Moderated by DHS, panelists included the Internet Security Alliance, Dickstein Shapiro LLP (a law firm that advises SAFETY Act applicants), Verizon, and Boeing. Panelists discussed questions related to the current environment in non-regulated sectors, whether research and development tax credits accessible to regional clusters and patent protection would be effective incentives, and how a risk-based approach should operate within the Framework.

Session III's cross-sector incentives panelists answered questions about their views on creating a competitive advantage for organizations seen as good stewards of cybersecurity, as well as how the Framework should address "signature-less" attacks. This panel was moderated by DHS and included panelists from SAIC, DHS, the General Services Administration, Northrop Grumman, and General Electric.

Session IV, the concluding government roundtable, provided participants with an opportunity to hear from the Federal representatives responsible for drafting the incentives studies for their respective Government departments. It consisted of DHS, the Department of Commerce, and the Department of the Treasury.

2.4.3. Department of Commerce Notice of Inquiry

On March 28, 2013, the Department of Commerce issued a 30-day Notice of Inquiry (NOI) entitled, "Incentives to Adopt Improved Cybersecurity Practices."[17] "Comments on Incentives to Adopt Improved Cybersecurity Practices NOI" were posted on April 29, 2013, and included 45 comments from the following 45 respondents:[18]

Advanced Cybersecurity Center, American Association for Laboratory Accreditation, American Fuel and Petrochemical Manufacturers, American Gas Association, American Insurance Association, American Petroleum Institute, American Public Power Association, atsec, Booz Allen Hamilton, Bryan Rich, Business Software Alliance, CACI, Covington & Burling/Chertoff Group, DCS Corp, Donald Edwards, Dong Liu, Edison Electric Institute, Electric Power Supply Association, Emmanuel Adeniran, Encryptics, Federal Communications Commission, Financial Services Sector Coordinating Council, Gary Fresen, Honeywell, Internet Infrastructure Coalition, Internet Security Alliance, IT SCC, Los Angeles Department of Water and Power, Marsh, Microsoft, Monsanto, National Cable and Telecommunications Assoc., NCTA- The Rural Broadband Association, National Electrical Manufacturers Association, National Rural Electric Cooperative Association, Robin Ore, San Diego Gas & Electric and Southern California Gas Company, Sasha Romanosky, Southern California Edison, Telecommunications Industry Association, Terrence August & Tunay Tunca, U.S. Chamber of Commerce, US Telecom Association, Utilities Telecom Council, and Voxem Inc.

As noted above, responses to the Commerce NOI were reviewed as a complement to the findings from the literature review, and to help inform conclusions about differences among evaluations as well as evaluations that are inconclusive. Similar to the DHS Incentives Workshop, the evaluation of NOI responses focused on the following questions:

[17] Docket number 130206115-3115-01: http://www.ntia.doc.gov/federal-register-notice/2013/notice-inquiry-incentives-adopt-improved-cybersecurity-practices
[18] The full responses can be accessed at: http://www.ntia.doc.gov/federal-register-notice/2013/comments-incentives-adopt-improved-cybersecurity-practices-noi

- Are there additional incentive categories, or sub-categories, that should be considered?
- Which incentives are most likely and least likely to promote adoption of the voluntary Framework and why?

Appendix 3.4 provides both a brief summary of the 45 responses to the Commerce NOI as well as a table that indicates which of the incentives considered were recommended, discussed, or neither discussed nor recommended by each of the respondents.

2.5. Finalization of the List of Incentives

Based on information and feedback obtained through the literature review, the DHS Incentives Workshop, and the Commerce NOI, the initial list of incentives was refined prior to conducting the analysis. Table 2 below summarizes both the initial list of incentives described above and the finalized list of refined incentive categories that were used as the primary units of analysis.

***Table 2.** Finalization of the List of Incentives*

	Initial Incentive Category		Final Incentive Category
1	Expedited Security Clearance Process	→	Remove due to existing DHS efforts
2	Grants		No Change
3	Include Cybersecurity in Rate Base	→	"Rate-Recovery for Price-Regulated Industries"
4	Information Sharing	→	Remove due to EO Section 4
5	Insurance	→	Remove as independent category and include in "Bundled Insurance Requirements, Liability Protections, and Legal Benefits"
6	Liability Considerations and Legal Benefits	→	Remove as independent category and include in "Bundled Insurance Requirements, Liability Protections, and Legal Benefits"
7	New Regulation/Legislation (e.g. "Cyber SAFETY Act")	→	Limit to "Bundled Insurance Requirements, Liability Protections, and Legal Benefits"
8	Prioritized Technical Assistance		No Change
9	Procurement Considerations		No Change
10	Public Recognition		No Change
11	Security Disclosure		No Change
12	Streamline Information Security Regulations		No Change
13	Subsidies		No Change
14	Tax Incentives		No Change

Expedited Security Clearance Process was removed from consideration due to existing DHS efforts to provide expedited clearances independent of adoption of the Cybersecurity Framework. More specifically, the DHS Critical Infrastructure Private Sector Clearance Program was developed in 2007 to facilitate the processing of security clearance applications for private sector partners. The DHS Office of Infrastructure Protection is implementing an improved process to streamline the clearance process and to meet the requirement in EO

13636 Section 4(d): "The Secretary… shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order." In doing so, DHS believes that national security should be the principal criteria for expediting clearances. Similarly, information sharing was removed as an incentive that would have been contingent upon adoption of the Framework due to the requirements in EO 13636 Section 4, which was interpreted to indicate that information sharing should occur independent of adoption of the Cybersecurity Framework.

The initial incentive, "Include Cybersecurity in Rate Base" was more clearly defined as "Rate-Recovery for Price-Regulated Industries," since price-regulated industries are the only industries to which rate-recovery of cybersecurity costs is able to be applied.

Both "Insurance" and "Liability Considerations and Legal Benefits" were removed as independent categories and were included in a bundle of insurance requirement, liability protections, and legal benefits, which would likely require legislation. DHS believes it is important to treat these incentives as a package, with each component an essential piece of a potential incentive structure. DHS believes that insurance is an important incentive independent of government intervention, and existing cybersecurity insurance markets may ultimately have the effect of promoting adoption of the Cybersecurity Framework outside of government intervention. For example, critical infrastructure owners and operators who adopt the Framework are likely to have lower levels of cybersecurity risk given their use of the standards, methodologies, procedures, and processes that will comprise the Cybersecurity Framework. If cybersecurity insurance premiums reflect the reduction in risk associated with Framework adoption, then the Framework and the cybersecurity insurance markets are likely to be mutually reinforcing: insurance will be more affordable for Framework adopters, and thus the probability of Framework adoption will be greater for those owners and operators who seek such affordable insurance policies. The incentive provided by lower premiums requires no government intervention beyond the planned development of the Cybersecurity Framework, and so there are no insurance actions to recommend within the scope of this report independent of the bundled incentive composed of insurance requirements, liability protection, and legal benefits. Nonetheless, market-based incentives like insurance can be encouraged via government policy, including policy that promotes sustained stakeholder dialogue about enhancing their viability. These incentives are encouraged through the bundled incentive requirements considered for this study: that owners and operators carry insurance in order to receive its liability protections.

2.6. Application of the Microeconomic Model

EO 13636 requires DHS to include an analysis of the benefits and relative effectiveness of the incentives considered. As described above, effectiveness is defined in terms of the probability of Framework adoption. To help distinguish between areas where incentives are assessed to have similar relative effectiveness, DHS also assessed each incentive in terms of two additional criteria that include benefits beyond the extent to which the incentive promotes adoption of the Framework: efficiency and equity. In general terms, each of these criteria answer the following questions:

- Effectiveness: Does it work?
- Efficiency: Is there waste?
- Equity: Who pays and how much?

To assimilate the broad range of information sources gathered in our research in an integrated analysis, each incentive was qualitatively assessed in terms of its relative effectiveness, efficiency, and equity. The incentives were then assessed in relative terms against each of these criteria using the following simple tiering heuristic:

- Top tier incentive, relative to other incentives, against each criterion
- Second tier incentive, relative to other incentives, against each criterion
- Insufficient evidence to merit either a top tier or a second tier assessment, relative to other incentives, against each criterion.

The efficiency criterion was only applied to the cost-sharing incentives.

2.6.1. Effectiveness: Does it work?

As described above, effectiveness is defined by the extent to which an incentive affects the probability of Framework adoption. Recall that the attributes in the microeconomic model that define the marginal benefit of Framework adoption are uncertain: Increasing unknown, and to some extent unknowable, benefits could increase the probability of adoption for some Framework adopters, while reducing Framework implementation costs that will occur with certainty increases the probability of Framework adoption for all Framework adopters. Additionally, marginal revenue increases would apply only to the subset of organizations that both adopt the Framework and sell goods and services to the Federal Government through the procurement process.

For these reasons, other things being equal, incentives that minimize the marginal increase in cybersecurity costs required to adopt the Framework through cost sharing are more likely to promote the adoption of the Framework than incentives that increase the perceived expected loss avoided by Framework adoption and/or that increase marginal revenue or ancillary benefits. As a result, effectiveness judgments are principally driven by Framework cost sharing, though expected loss avoidance, marginal revenue increase, and ancillary benefits also contribute to a lesser extent.

The incentives that minimize the marginal increase in cybersecurity costs required to adopt the Framework through cost sharing include:

- Grants,
- Rate-recovery for price-regulated industries,
- Subsidies, and
- Tax incentives.

Of these four categories, two incentives are assessed to be in the top tier of incentive categories for cost-sharing, and thus the top tier of incentive categories for the probability of Framework adoption: grants to non price-regulated industries, and rate-recovery for price-regulated industries. Subsidies and tax incentives are assessed to be in the second tier for cost-sharing and thus the second tier for the probability of Framework adoption.

This is in part due to the temporal nature of the cost-sharing provided by each of these incentives. Both grants and price-caps are able to help offset the costs of Framework adoption before those costs are incurred. Tax incentives would provide either full or partial reimbursement for costs that have already been incurred. For those organizations for which operating cash flows are insufficient to support non-operating costs, offering reimbursement for costs incurred to adopt the Cybersecurity Framework may be insufficient to spur the required investment. However, grants, subsidies, and tax incentives create a potential moral hazard where taxpayers fund cyber security improvements for privately owned critical infrastructure, potentially for the long-term.

A recent study summarized the existing research on the effectiveness of R&D tax incentives and reported that, “while there is substantial evidence that R&D tax incentives increase the level of [measured] R&D,” there is “scarce evidence, however, that even the most successful innovation tax incentives are cost-effective.” For example, they cite a benefit-cost ratio of between 0.293 and 2.0 and remark that any particular incentive could have widely varying effects, depending on firm size, the time frame, and other factors. A separate study found a

price elasticity of 3 to 4 for changes in state R&D tax incentives, and GAO found that the gains in R&D spending were only a fraction of the cost of the credit.

Subsidies in the form of payments for reported expenses would provide either full or partial reimbursement for costs that have already been incurred. In the case of an interest subsidy, the costs could be offset temporarily in the form of a subsidized loan before the Framework costs are incurred. Additionally, an interest rate subsidy could create an unintended incentive for owners and operators to take on debt.

Due to the volume of the literature reviewed, a summary of the literature on effectiveness is contained in Appendix 3.1 and the relevant references are listed in Appendix 3.2.

2.6.2. Efficiency: Is there waste?

Efficiency was applied to cost sharing incentives and consists of both moral hazard and adverse selection. Moral hazard in this context exists because of differences in the degree to which techniques for adopting the Framework are cost-effective, and can be thought of as allowing owners and operators to choose techniques that are not cost-effective. Adverse selection in this context exists due to differences in the cost of adoption among owners and operators within and across sectors, and can be thought of as over-paying "lost cost" owners and operators that are already near the frontier of sophistication.

The efficiency criterion was only applied to the four categories of cost-sharing incentives: grants to non price-regulated industries, and rate-recovery for price-regulated industries, subsidies, and tax incentives. Of these, based on both economic theory and evidence in the literature, the following two incentives are assessed to be in the top tier for efficiency because they address both moral hazard and adverse selection: grants to non price-regulated industries, and rate-recovery for price-regulated industries.

As noted in the previous section, due to the volume of the literature reviewed, a summary of the literature on efficiency is contained in Appendix 3.1 and the relevant references are listed in Appendix 3.2.

2.6.3. Equity: Who pays and how much?

Each of the incentives was also assessed in terms of (1) whether government, industry, or consumers would pay for the cost of Framework adoption and/or the administration of the incentive, and (2) whether they would pay all/most of the cost of Framework adoption and/or the administration of the incentive, a moderate amount, or none/least.

The incentives for which the government or taxpayers would bear none or the least cost for Framework adoption and administration of the incentive are: rate-recovery for price-regulated industries, prioritized technical assistance, procurement considerations, and streamlining information security regulations. From a policy-making perspective these incentives are considered more equitable. Due to programmatic costs associated with administering the incentives, government and taxpayers would bear a moderate portion of the cost of the Bundled Insurance Requirements, Liability Protections, and Legal Benefits; Public Recognition; and Security Disclosure. Grants to price-regulated industries, subsidies, and tax incentives would require government and taxpayers to pay most or all of the cost of Framework adoption.

By definition, industry would bear none or the least cost for Framework adoption for the four categories of cost-sharing incentives: grants to price-regulated industries, rate-recovery for price-regulated industries, subsidies, and tax incentives. Industry would bear a moderate portion of the cost of Framework adoption for the Bundled Insurance Requirements, Liability Protections, and Legal Benefits: its insurance requirements and application process would impose some level of transaction costs, while the risk transfer it provides through insurance and liability protections would help to offset expected losses incurred by cybersecurity incidents. Industry would bear all or most of the costs of Framework adoption for the remaining incentives: prioritized technical assistance,

procurement considerations, public recognition, security disclosure, and streamlining information security regulations.

Finally, consumers of the products and services provided by owners and operators (as distinct from the general class of taxpayers) would bear none or the least cost for Framework adoption for grants to price-regulated industries, prioritized technical assistance, public recognition, streamlining information security regulations, subsidies, and tax incentives. Consumers would bear a moderate portion of the cost for the Bundled Insurance Requirements, Liability Protections, and Legal Benefits, procurement considerations, and security disclosure, since the cost of insurance premiums, procurement requirements, and security disclosures are likely to be passed on to consumers through the price of the goods and services consumed. By definition, consumers would bear all or most of the cost of rate-recovery for price-regulated industries.

2.6.4. Analytic Summary

Figure 2 below summarizes the analysis of each of the incentives against the criteria above.

Figure 2. Analytic Summary

	Incentive	Effectiveness				Efficiency		Equity		
		Probability of Framework Adoption	Framework Cost Sharing	Expected Loss Avoided	Marginal Revenue Increase and Ancillary Benefits	Moral Hazard	Adverse Selection	Government/ Taxpayer Cost	Industry Cost	Consumer Cost
1	Grants	●	●			●	●		●	●
2	Rate-Recovery for Price-Regulated Industries	●	●			●	●	●	●	
3	Bundled Insurance Requirements, Liability Protections, and Legal Benefits	○		●				○	○	○
4	Prioritized Technical Assistance			○				●		●
5	Procurement Considerations	○			●			●		○
6	Public Recognition							○		●
7	Security Disclosure							○		○
8	Streamline Information Security Regulations				○			●		●
9	Subsidies	○	○				●		●	●
10	Tax Incentives	○	○				●		●	●

Key

●	Indicates a top tier incentive, relative to other incentives, against the criterion defined *within* each column.
○	Indicates a second tier incentive, relative to other incentives, against the criterion defined *within* each column.
	Indicates insufficient evidence to merit a top tier or a second tier assessment, relative to other incentives, against the criterion defined *within* each column.
▒	Indicates the criteria were not applied to the incentive.

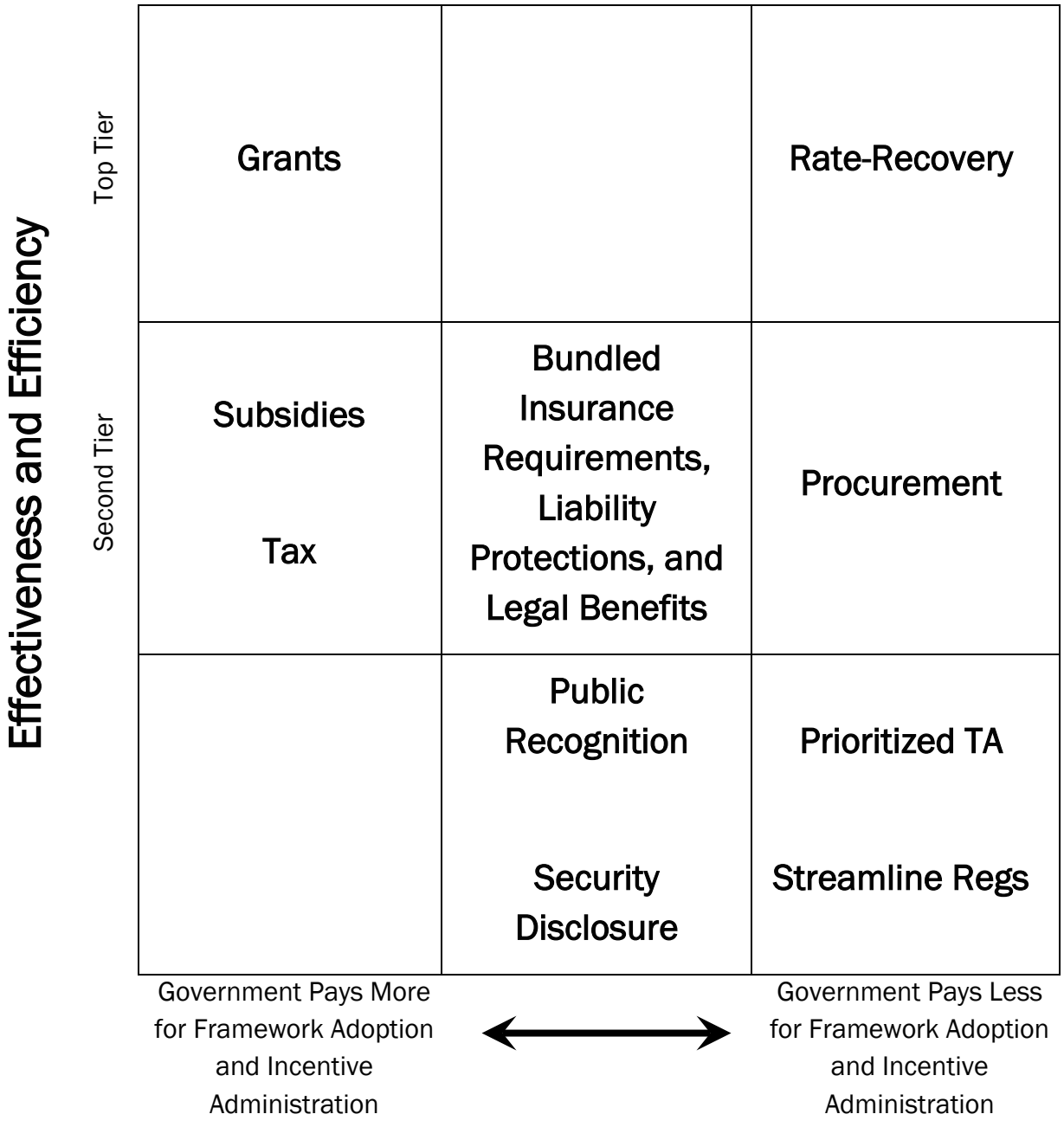
The analysis of effectiveness, efficiency, and equity summarized in Figure 2 includes nine dimensions of economic criteria, and three tiers of assessment for each of ten incentive categories, resulting in 78 data points. Since the purpose of this analysis is to help inform the decision about which incentives to implement to promote adoption of the Cybersecurity Framework, a method for applying this analysis in a way that synthesized the 78 data points was needed to generate meaningful findings that allowed for consideration of the tradeoffs that reflected the decision to be informed. The method that was selected was to reduce the dimensionality of the criteria through two consolidations.

First, as noted in Section 2.6.2, the efficiency criterion was only applied to the four cost-sharing incentives: grants to non price-regulated industries, rate-recovery for price-regulated industries, subsidies, and tax incentives. Of these, the top tier for both effectiveness and efficiency included the same two incentives: grants to non price-regulated industries, and rate-recovery for price-regulated industries. The second tier for both effectiveness and efficiency similarly included the same two incentives: subsidies and tax incentives. As a result, the effectiveness and efficiency criteria were consolidated as follows: for those incentives for which efficiency was applied, the top and second tiers for the consolidated criteria were the same as either criterion individually. For those incentives for which efficiency was not applied, all tiers for the consolidated criteria were assessed to be the same as the effectiveness criteria alone.

Second, it was assumed that an important decision point for the selection of the incentives for implementation will be the degree to which new government funding is available. Accordingly, the dimensions for the equity criteria were reduced from three to one by focusing the equity analysis only on government/taxpayer costs.

The analytic application of these consolidations resulted in the three-by-three matrix shown in Figure 3 below, with the consolidated tiering assessment for effectiveness and efficiency on the y-axis. The x-axis represents a range, from left to right, from government/taxpayers pay more for Framework adoption and incentive administration to government/taxpayers pay less for Framework adoption and incentive administration.

Figure 3. Consolidated Analysis



3. APPENDICES

3.1. Literature Review[19]

3.1.1. Grants, Rate-Recovery, and Subsidies

The question of how to best incentivize investment in cyber security falls into the broader study of how to design effective economic incentive mechanisms. The most effective incentives overcome both moral hazard and adverse selection – which arise from information asymmetry. This section reviews economic literature related to common economic incentive mechanisms.

Moral Hazard. A variety of techniques exist to incentivize firms to achieve cyber security standards. The firms responsible for critical infrastructure are in the best position to determine which techniques are most cost-effective since costs depend on a host of factors specific to individual firms. Moreover, even if the government knew the best techniques to achieve its cyber security standard, it may be difficult or costly to monitor those chosen by each firm. This problem is called "moral hazard" and arises from information asymmetry – meaning the firms know more about the costs of meeting the cyber security standard than the government.

The presence of moral hazard calls for policy incentives that enable firms to profit from taking cost-saving actions. For example, the government could provide fixed grants contingent upon a firm meeting its cyber security standard. Since the grant would depend only on meeting the standard and not on the techniques used to meet it, the firm would have a powerful incentive to find the most efficient techniques.

This basic principle has been applied in numerous settings including the regulation of public utilities, government contracting and various research prizes:

Since the 1980s, government regulation of public utilities has increasingly moved from traditional "rate-of-return" regulation to "price cap" regulation. Under rate-of-return regulation, the price a firm is permitted to charge consumers varies positively with the firm's cost. This guarantees firms a fixed rate of return and provides little incentive to save on costs. In contrast, price cap regulation sets a fixed price for consumers, enabling firms to increase profits by reducing costs. Price cap regulation is common in the context of electric distribution and transmission networks (Joskow, 2013) and telecommunications (Sappington, 2003) – see Vogelsang (2002) for more examples. Joskow (2013) shows empirical evidence that the introduction of price caps led to substantial cost reductions in the electric distribution and transmission networks of the United Kingdom.

In addition to public utilities, similar policy incentives exist in government grants. The government grants process has seen an increased use of performance-based [as opposed to cost-based] procurement arrangements. A recent variant is the "pay for success" model of delivering social services. In the pay-for-success model, a government agency commits funds to pay for a specific outcome achieved within a given period of time. The financial capital to cover the operating costs of achieving the outcome is provided by independent investors – however, the government disperses payment of the funds contingent on the specified results. Similar to price cap regulation, investors have an incentive to provide a successful program at the lowest cost. The pay-for-success model is being tried in several states and has been included in the last three of the President's Budgets. Mulgen, et. al. (2011) provides an extensive discussion of the principles behind, and the nuances in implementing, pay-for-success programs. Notably, they require careful and objective measurements of success.

Lastly, various research prizes, such as those recently offered by the X-Prize Foundation, have been successful in spurring innovation in socially desirable directions. Kremer and Williams (2010) discuss these prizes, including

[19] As noted in Section 2.4.1, the review of the relevant literature was supported by the White House Council of Economic Advisers, the Department of the Treasury's Office of Tax Policy and Federal Insurance Office, and the Homeland Security Studies and Analysis Institute.

the recent $1.5 billion pilot Advance Market Commitment (AMC) mechanism for a pneumococcus vaccine. Under an AMC, the sponsor legally commits—in advance of product development and licensure—to underwrite a guaranteed price for a vaccine. Vaccines are eligible if a committee deems that they fulfill a set of technical specifications laid out in advance.

Unobserved Heterogeneity of Costs. Even with the most efficient techniques, there are wide disparities between firms within and across industries in terms of the cost of meeting the standard. The government may not know the full extent of these cost disparities when it issues incentives, which makes it difficult to tailor them to appropriate firms. For example, if the government could anticipate how much it would cost each firm to achieve the standard, it could tailor the incentives to cover only the cost of achievement. This would ensure the standard's adoption by all firms at the lowest cost to taxpayers. The only way to induce widespread adoption of the standard when cost disparities are unknown is to offer incentives generous enough to cover the highest-cost firms. It is likely that the incentive will exceed the amount needed to cover low-cost firms, consequently wasting public funds. This problem is known as "adverse selection" and like moral hazard, arises from asymmetric information.

If the government could observe the cost of adopting cyber security standards after each firm had incurred its expenses, then a potential solution to adverse selection is a cost-sharing system. Under a cost-sharing system, the government only pays for costs incurred by firms to reach the standard. Examples include subsidies and tax credits based on a firm's reported cyber expenses. Such policies are equivalent to the rate-of-return regulation discussed previously in the context of regulated utilities. Both policies suffer the same problem: while they avoid over-paying low cost firms, they blunt the incentive to take cost-saving actions –which is necessary for overcoming moral hazard. It may also be difficult to determine which of a firm's expenses were necessary to meet the standard and which would have been made regardless. For example, tax credits and subsidies end up paying for work that would have been done anyway. For these reasons, a cost-sharing system is not the recommended approach.

Various approaches to solving the trade-off between moral hazard and adverse selection have been advanced in both theory and practice. Laffont and Tirole (1986) argue that the tradeoff can be solved by offering firms a "menu" of incentive schemes. While the exact nature of the optimal menu is complex, Rogerson (2003) shows that the idea can be implemented by offering firms a choice between a cost-reimbursement contract and a fixed-price contract. A low-cost firm is likely to choose the fixed-price contract with the concomitant incentive to choose efficient techniques. A high-cost firm is likely to choose cost-reimbursement.

The most common approach in the context of utility regulation is to choose a price cap based on historical or constructed data that firms cannot manipulate by incurring unnecessary costs (Joskow, 2013; Vogelsang (2002). The goal is to choose a firm-specific price cap that leaves as little profit for the firm as possible while not depending on the behavior of the firm itself. If the price cap depends on a firm's behavior, (i.e., if this year's price cap depends on last year's realized cost) firms have an incentive to distort their behavior to raise their realized cost. A common approach begins with a historical base-line cost and then adjusts annually for: inflation, some "x-factor" reflecting efficiency improvements, and a "y-factor" accounting for changes in input prices beyond the firm's control. Another approach is known as "yardstick competition," whereby each firm's price cap depends on the cost of its competitors.

A third option would be to rely on gradations of performance and tie incentives to cyber-security improvements. It goes without saying that any scheme tying incentives to compliance must be monitored to verify that a firm has complied with the standard. Ideally, the monitor would measure gradations of compliance, rather than using binary measure (compliant or not). Examples of this include Energy Star ratings and DHS SAFETY Act certifications/designations. Similar to the "pay for success" model, the payment firms receive could escalate with improvements in cyber-security.

Such an approach could go a long way toward solving the adverse selection problem. Under a program that rewards only full compliance, a high-cost firm would require a large payment before it would be willing to make an effort. The same firm would be more likely to make an effort if it were rewarded for improvements. By the same token, low cost firms would likely begin the program with high grades and thus be able to obtain only limited payments for improvement before hitting full compliance (though one may want to incorporate some penalty for backsliding).

Regulated Firms. Many of the critical infrastructure sectors identified as "lifeline" sectors (i.e. electricity, water, transportation, and communications/IT) involve price-regulated firms, so that the adoption of a cyber-security standard can be grafted onto existing incentive regulation. A firm operating under a price cap already faces a high-powered incentive to minimize costs. If the government also wanted the firm to adopt a cyber-security standard using the lowest-cost technique, this could be accomplished by raising the price cap, contingent on the firm improving (or meeting the standard), by an amount that would be sufficient to cover additional cost.

3.1.2. Insurance

Cybersecurity insurance transfers risk from individuals and organizations to insurance carriers. It can help mitigate losses due to data breaches, network damage, or cyber extortion. However, risk managers recommend that a risk transfer strategy be pursued only after other risk management strategies (i.e., risk acceptance, risk mitigation, and risk avoidance) have been exhausted (DHS, 2012). In addition to general insurance problems such as moral hazard—in which the availability of insurance protection increases risky behavior—the literature suggests certain challenges faced by the use of insurance to promote cybersecurity. Moore (2010) and Lelarge and Bolot (2009) cite the current (when their articles were written) lack of data for cyber damages as a specific difficulty for cyber insurance implementation; without reliable estimates of incident damage, appropriate insurance premiums cannot be determined to properly align incentives. At a Department of Homeland Security (DHS) Cybersecurity Insurance Workshop held in October 2012, an IT professional stated that the data needed by insurers to understand the risks and economics of this threat are in short supply, limiting the availability and breadth of policies. However, another workshop participant responded that this data exists but "few [companies] have interpreted that data to clarify their potential losses and corresponding insurance needs," in part because they do not know that affordable and attractive cybersecurity insurance policies exist and also because of their reluctance to share cyber incident data with the public. Moore (2010) also points out entities' lack of awareness of cyber-risk as an issue, but insurers suggest mandatory security breach disclosure legislation to help overcome this.

That said, insurance can offer incentives for firms or individuals to invest in cybersecurity by providing lower premiums for those entities that take the appropriate precautions. Hahn and Layne-Farrar (2006) "see cyber insurance as an extremely promising route to solving the identified market failures in software security."

In 2002, Kunreuther established that there is a "lack of interest by insurers, reinsurers and investors in providing funds for protection against terrorist attacks." With the passage of the Terrorism Risk Insurance Act of 2002, the United States established a public-private partnership in which the government provides no-cost reinsurance to insurers. Michel-Kerjan and Raschky (2011) use empirical evidence to shows that government intervention in this market has impacted insurers' behavior, finding "tentative evidence for moral hazard caused by the government backstop under TRIA."

Due to the limited academic literature on cyberinsurance, we are unable to determine the effectiveness of cyberinsurance as an incentive to induce firm behavior. However, research attempts to determine if insurance affects internet security. For example, Lelarge and Bolot (2009) study the benefits of using insurance to manage internet risks. They conclude that insurance can increase the level of self-protection and overall security of the internet. This stands in sharp contrast to the claims of Sheety, Schwartz, Felegyhazi, and Walrand (2010), who

also seek to determine the effects of cyber insurance; their model concludes that while insurance improves user welfare in general, it fails to improve network security. Beyond cybersecurity, insurance is a tool that can be used to induce risk-mitigating behavior. Landry and Li (2012) conduct a study focused on factors contributing to the adoption of a hazard mitigation project, as reflected in Community Rating Systems participation, which offers flood insurance discounts based on management activities. They find empirical evidence that previous flood experience increases participation; however, results were mixed for the impact of flood events when looking across time.

3.1.3. Liability and Legal Benefits

Legal incentives can be used to motivate socially optimal behavior (through "carrot" incentives like liability protections) and deter harmful behaviors (through "stick" incentives like liability standards). The research suggests that legal incentives can be an effective policy tool for environmental programs, but their degree of effectiveness varies by firm- and industry-specific factors.

For example, Alberini et al. and Turvani (2005) and Wernstedt, Meyer, and Alberini (2006) find that real-estate developers with potential interest in brownfield properties value liability relief as an incentive, refuting earlier claims (Urban Institute et al, 1997) that developers do not value liability relief as an incentive. Both Alberini et al. (2005) and Wernstedt et al. (2006) find that inexperienced developers are more responsive to liability relief than other forms of incentives, although this may only apply to the subpopulation of inexperienced developers that are reasonably likely to consider investing in brownfield projects. Alberini et al. (2005) also find that developers who sell their development projects, as opposed to using them, appear to value liability relief even more highly.

Alberini and Frost (2007) suggest that economic theory is ambiguous on predicting the response of a firm handling hazardous waste in a state with a strict liability standard. Shavel (1984) finds that "strict liability forces a firm to internalize pollution damage and choose [to take greater care] against accidental releases" but only if damages of pollution do not exceed the firm's assets. However, Beard (1990) finds that "when the damage exceeds the firm's assets or the firm can escape prosecution, it will take less precaution." Alberini and Austin (1999) find empirical evidence that "strict liability may, in fact, increase [emphasis added] the frequency of accidental releases of toxic pollutants" for firms holding specific types of chemicals, but state that further research is needed to understand why this occurs.

Tietenberg (1989) suggests that it appears the effects of liability laws vary with the scale and the assets of the firm that generates waste. Alberini and Austin (1999) find evidence that smaller firms find shelter from liability laws due to their limited assets (i.e., they avoid "wealth targeting" by regulatory agencies), and as a result, they are disproportionately responsible for spills or accidents in states imposing strict liability on polluters.

3.1.4. Prioritized Technical Assistance

Research identified limited literature on prioritized technical assistance as an incentive to induce firm behavior; therefore, its effectiveness as an incentive remains unclear. However, the two studies cited below point to its potential ineffectiveness.

Johnston (2005) studies the Strategic Goals Program, a voluntary environmental program for job shop metal finishers, and finds that direct technical assistance "was insufficient to enlist large numbers of the important middle tier firms." However, the study suggests that technical assistance provided value to smaller firms by offering knowledge that increased profitability.

The Malaysian government introduced three incentives, including a fast track approval process, to encourage developers to implement a new housing delivery system, Build Then Sell (BTS). Yusof, Abu-Jarad, and Badree (2012) find that these "incentives are ineffective to influence the implementation of BTS."

3.1.5. Procurement

The government can use preferential consideration in the procurement process to promote participation by disadvantaged enterprises, such as small or minority owned businesses. In general, the literature appears to suggest that procurement preference can motivate firm behavior. For example, Myers and Chan (1996) and Chatterji, Chay, and Fairlie (2013) examine the effectiveness of preferential treatment for minority businesses. Myers and Chan find that preferential treatment increased the number of bids submitted by minority businesses; this corresponds with a reduction in their success rates as the total number of bids did not increase. Similarly, Chatterji et al. note an increase in African-American business ownership rates after implementation of a preferential program. Kranokutskaya and Seim (2011) look at preferential treatment of small bidders in highway procurement auctions and its effect on their incentives to participate in government procurement. They find that the bid preference "has significant implications for [small bidders'] participation and bidding behavior" and the program has been successful in promoting participation by disadvantaged enterprises. However, this preferential treatment comes at a cost to the government as allocation of bids moves away from the lowest cost competitors in the market.

In addition to procurement considerations for minority groups, the government uses preferential treatment to promote environmentally responsible firms. After assessing green public procurement (GPP) as a policy tool, Brannlund, Lundberg, and Marklund (2009) find that "even if firm type tailored criteria would be allowed, the possibility for GPP to work as a cost-efficient environmental policy tool is still negligible in practice;" therefore, other tools, such as taxes, are preferable.

3.1.6. Public Recognition

The literature is inconclusive on the effectiveness of public recognition to induce firm behavior. However, public recognition offered by voluntary programs can be attractive to potential participants as a signal of quality to the marketplace. For example, Videras and Alberini (2000), Arora and Cason (1996), and Brouhle and Harrington (2010), find that public recognition is an important component of participation in voluntary environmental programs. Specifically, Videras and Alberini (2000) note that "firms who wish to show consumers about their environmental performance progress and who do so by publishing environmental reports" are more likely to participate. Arora and Cason (1996) find that larger firms, those with greatest toxic releases, and those with higher advertising expenditures are more likely to participate. Gugerty (2009) examines motivations of non-profits for joining voluntary accountability and standard-setting programs. He indicates that "club theory and the economics of certification suggest that such programs have the potential to provide a signal of quality by setting high standards and fees and rigorously verifying compliance." Karamos's (1999) study on identifying the characteristics and incentives that induce company participation in Voluntary Environmental Agreements (VEAs) provides a literature review indicating that public recognition is one of the two most prevalent incentives linked to participation in the Department of Energy's Climate Challenge Program (CCP).

Brouhle and Harrington (2010) find evidence that firms use participation in voluntary environmental programs to signal to investors and regulators but not to consumers. Using survey data for a sample of S&P 500 firms, Khanna and Anton (2002) conclude that public recognition of firms who adopted environmental management systems allows differentiation from other firms. Additionally, market pressures by consumers, investors, and competitors create greater incentives for adoption than other instruments such as the threat of liability or mandatory regulation.

Banerjee and Solomon (2003) study the effectiveness of five energy-labeling programs, including government and private sector initiatives. They find that "[g]overnment support to a labeling program not only increases its credibility and recognition, but also improves financial stability, legal protection and long-term viability" and that

"[s]imple seal-of-approval logos and labels have generally affected consumer behavior more than the complex information-disclosure labels."

3.1.7. Security Disclosure

Security disclosure in the cybersecurity field could encourage companies to better secure the personal information they hold about individuals and take steps to prevent the breaches that cause them. While security disclosure may indeed promote such benefits, for the purpose of this study effectiveness was evaluated as the ability to promote adoption of the Framework. Security disclosure as an incentive for Framework adoption could be implemented in one of two ways: (1) apply disclosure laws to any organization that is the victim of a security disclosure breach, or (2) require owners and operators that do not adopt the Framework to disclose security breaches, and do not require owners and operators that do adopt the Framework to disclose security breaches.

Under the first method, to avoid the negative reputational effects that security disclosure would impose, owners and operators would be motivated to adopt those portions of the Framework that would mitigate future security breaches. Since the extent to which the Framework will address security breaches is unknown, it is unclear whether this would constitute a large or small portion of the overall Framework. Under the second method, adverse selection would encourage those firms most likely to have security breaches to adopt the Framework, and the resultant perverse incentive would be greater adoption of the Framework among those "breach-likely" firms and underreporting of breaches and perhaps their mitigation. For these reasons, security disclosure is not assessed to be in one of the top tiers of effectiveness for Framework adoption.

Nonetheless, if security disclosure were considered independent of Framework adoption, the review of the relevant literature that follows indicates that, overall, disclosure can be an effective motivator of firm behavior across various regulated industries. In some industries, government bodies have been able to create incentives for companies to protect citizens simply by providing greater disclosure of practices. For example, a meta-analysis conducted by Weil, Fung, Graham, and Fagotto (2006) assess the effectiveness of what they call "regulatory transparency systems" (mandatory disclosure of information by private or public institutions with a regulatory intent) in restaurant hygiene, nutritional labeling, workplace hazard communication, and five other diverse systems in the U.S. Their two main conclusions indicate:

- "transparency systems alter decisions only when they take into account demanding constraints by providing pertinent information that enables users to substantially improve their decisions with acceptable costs." The presence of this phenomenon is referred to as "user embeddedness."
- "highly effective transparency policies … cause users to systematically incorporate new responses into their decision making that in turn change disclosers' decision calculations." The presence of this phenomenon is referred to as "discloser embeddedness."

Disclosure mechanisms are used in a variety of industries, with varying levels of influence on firm behavior. On restaurant hygiene, Jin and Leslie (2003) find that hygiene grade cards displayed in restaurant windows caused restaurants in Los Angeles County to improve hygiene quality and led to "possibly a 20 percent decrease in food-related hospitalizations." A similar study by Simon et al. (2005) determines there was a 13 percent decrease in the number of foodborne disease hospitalizations in L.A. County in 1998, the year following the implementation of the hygiene grade program. Findings by Jin and Leslie (2009) support the view that "reputation can cause firms to provide safe products."

The literature suggests that disclosure mandated by legislation can induce socially optimal effects. For example, Bennear and Olmstead's (2008) study suggests the 1996 Amendments to the Safe Water Drinking Act, which mandated that community drinking water suppliers issue annual consumer confidence reports (CCRs) to customers, resulted in a reduction of "total violations between 30% and 44% … and reduced the more severe health violations by 40%-57%" for larger utilities required to mail CCRs directly to customers. Konar and Cohen

(1997) find that on the day following the issue of toxic release inventory (TRI) data to the public "firms with the largest stock price decline … subsequently reduced emissions more than their industry peers….[This] is consistent with the view that financial markets may provide strong incentives for firms to change their environmental behavior."

A study by Blackman, Darley, Lyon, and Wernstedt (2010) on Oregon's voluntary clean-up programs (VCPs) finds that public disclosure of contaminated sites spurs voluntary remediation by responsible parties. Chatterji and Toffel (2010) find that firms "shamed" by low KLD ratings—the most widely used rating of corporations' environmental activities and capabilities—were "most 'able' to seize low-hanging fruit [to] show the most improvements in environmental performance."

However, impact on consumer behavior due to nutrition labeling is less clear. Moorman (1998) finds that food companies strategically reacted to this new requirement by adding low-fat, low-sodium product choices, but not eliminating traditional unhealthy options. Research in this area indicates "positive results on public health are less clear (Derby and Levy, 2001)." Weil et al. (2006) find that the following disclosure systems produced moderate or low effectiveness: toxic releases, workplace hazards, patient safety, and plant closing notification.

Dalley's (2007) examination of regulators' use of disclosure schemes rather than substantive regulation over the past several decades to achieve regulatory goals leads him to conclude that "only when one understands the mechanism by which the disclosure system will operate (i.e. accounting for how firms and individuals process and react to information) can one assess the likelihood that it will in fact achieve its goal and what the true costs of the disclosure requirement are."

3.1.8. Tax[20]

The following literature review presents a short description and bibliography of attempts within the professional literature to measure the effectiveness of two major types of tax incentives. This listing is not intended to be comprehensive. The first section discusses findings regarding the credit for increasing expenditures on research and development (R&D). The second section reviews papers that have estimated the effects of tax incentives on tangible, depreciable investments, especially those in equipment.

The Research Credit

Using a cost of capital approach in a multi-country regression analysis, Bloom and van Reenen (2002) find a short-run price elasticity for R&D activity of about -0.1, but a long-run elasticity of just under -1.0. They find that the variation between firms in the effectiveness of the credit depends on their different tax positions. The authors cite Baily and Lawrence (1992), Hall (1993), Hines (1994), and Mamuneas and Nadiri (1996) as also finding price elasticities of at least unity. They also cite Mansfield (1986) and Griffith, Sandler, and van Reenen (1995) as being perhaps more skeptical concerning the sensitivity of R&D to its user cost. Among other things, they refer to the possibility that taxpayers may be simply relabeling expenditures as R&D, as opposed to actually conducting greater R&D activities.

In a recent paper, Graetz and Doud (2012) summarize the existing research on the effectiveness of R&D tax incentives. They report that, "while there is substantial evidence that R&D tax incentives increase the level of [measured] R&D," there is "scarce evidence, however, that even the most successful innovation tax incentives are cost-effective." For example, they cite a benefit-cost ratio of between 0.293 (McCutchen (1993)) and 2.0 (Hall (1993)), and remark that any particular incentive could have widely varying effects, depending on firm size, the time frame, and other factors. Wilson (2009) finds a price elasticity of 3 to 4 for changes in state R&D tax

[20] As noted in Section 2.4.1, the review of the relevant tax literature was conducted by the Department of the Treasury's Office of Tax Policy, and is reproduced here in Appendix Section 3.1.8. as provided by that office.

incentives, but Graetz and Doud also cite the Bloom and van Reenen (2002) paper, as well as U.S. GAO (1998), which found that the gains in R&D spending were only a fraction of the cost of the credit.

Graetz and Doud question whether R&D incentives lead to increased output overall, or whether they simply shift R&D among regions. They cite a few conflicting studies in this regard. Cantwell and Mudambi (2000) suggest that incentives do not affect location decisions, but their study is limited to U.K. data only. Hines and Jaffe (2000) found evidence to suggest that domestic and foreign R&D are complements, while Wilson (2009) found the opposite result. Graetz and Doud also raise the possibility that companies reclassify expenditures to qualify for the incentives.

Finally, these authors report on several studies that have evidence concerning whether R&D has spillover effects or otherwise increases productivity. Lychagin et al. (2010) find positive effects in nearby locations, but that these effects decay rapidly with distance. Griffith, Redding, and van Reenen (2001) found that an R&D tax credit increases productivity, but that the increase is not cost effective in the short-run. The long-run could yield the opposite conclusion. Machin and van Reenen (1998) found that increased R&D increases the demand for skilled workers, while Goolsbee (1998a) found that incentives tend to increase the salaries of R&D workers rather than increase the volume or quality of R&D performed. Additional studies in this vein include Thomson and Jensen (2011) and Aerts (2008), which imply that incentives shift resources toward the employment of skilled workers and increase relatively the salaries of those already employed.

More recently, Rao (2013) has found a short-run user cost elasticity of about unity for qualified R&D spending (as a percent of sales), with larger effects in the long-run. Her work, however, suggests that much of the response may be due to a reallocation of spending between nonqualified and qualified research spending.

Investment Incentives

Most investment tax incentives aim to lower the user cost of new capital outlays and thereby increase the demand for investment. Hassett and Hubbard (2002) provide a history of theoretical and empirical developments in this area. After citing work by Auerbach and Hassett (1991), Caballero, Engel and Haltiwanger (1995), Cummins, Hassett and Hubbard (1994, 1996), and Goolsbee (2000), they conclude that empirical studies had "reached a consensus that the elasticity of investment with respect to the tax-adjusted user cost of capital is between 0.5 and 1.0." They also cite a finding by Goolsbee (1998b) of a significant response of capital goods prices to investment subsidies, concluding that capital goods manufacturers largely capture the benefits of investment tax incentives. However, the opposite conclusion is found in Hassett and Hubbard (1998), who find that local investment tax credits have had a negligible effect on (world) prices paid for capital goods.

Other work, including Eisner (1969), Summers (1981), Bernanke, Bohn, and Reiss (1988), and Chirinko, Fazzari, and Meyer (1999) has been less sanguine regarding the effects of tax variables on business investment. For example, using micro data, Chirinko, Fazzari and Meyer found a user-cost elasticity for equipment of -0.25. This may be compared to the -0.66 elasticity found by Cummins, Hassett, and Hubbard.

Hines(1998) argues that tax incentives for equipment investment could lower the pre-tax returns of such capital, reducing the payoffs to bondholders in case of bankruptcy, and that bondholders should demand that firms pay them higher interest rates to compensate for this risk. Hines found evidence consistent with this mechanism in studying the Tax Reform Act of 1986. Thus, it is possible that aggregate investment could fail to rise, even as favored assets are substituted for assets not so favored by the tax incentive. Other mechanisms may also affect both the micro and macro responses to the introduction of a major tax incentive.

Plummer (2000) looked at firm-specific forecasts of capital expenditures published before and after relevant tax legislation dates. She found the investment tax credit's incentive effects were concentrated primarily among low-debt firms and firms with positive taxable income.

Desai and Goolsbee (2004) found evidence of a larger responsiveness of investment to tax parameters. Consistent with the "new view" of dividend taxation, they also found that dividend taxes failed to influence incentives for making investments.

More recent estimates have focused on the reaction of equipment investment to temporary tax incentives, such as increased first-year write-offs (expensing). Such incentives have been in place for much of the past decade, but always on a temporary basis, with supposed known ending dates. The amount of increased expensing (when it has been in force) has varied between 30 percent, 50 percent, and 100 percent of an investment's cost. The main purpose of a temporary incentive is to alter the timing of investment over time – stealing from the future, so to speak, in order to generate aggregate demand currently. Desai and Goolsbee (2004) found that the effect of 30 percent partial expensing was too small to have a large impact. Cohen and Cummins (2006) found only a small response to the earliest expensing provision. Knittel (2007) found evidence that firms with losses and loss carryovers tended not to use the credit; the incentive of a faster write-off of investment cost was certainly lower for such firms. Also, a substantial number of states refused to align their income taxes with the federal system with regard to the expensing provision, creating a disincentive for taxpayers to use the expensing provision. A more recent study, House and Shapiro (2008), using the same data as Cohen and Cummins, found large differences in investment response across asset types that were differentially affected by the temporary expensing incentive.

Edgerton (2010) focused on the interactions of tax incentives with individual tax characteristics of firms, finding that financing constraints and tax carrybacks and carryforwards are important determinants of the effectiveness of investment tax incentives. His most salient finding was the importance of a company's cash flow on its ability to take advantage of tax incentives.

3.2. Bibliography

Aerts, K. 2008. “Who writes the pay slip? Do R&D subsidies merely increase researcher wages? Katholieke Universitiert Leuven, 33.

Alberini, Anna and Kathleen Segerson. 2002. “Assessing Voluntary Programs to Improve Environmental Quality.” Environmental and Resource Economics, 22: 157-184.

Alberini, Anna, and David H. Austin. 1999. “Strict Liability as a Deterrent in Toxic Waste Management: Empirical Evidence from Accident and Spill Data.” Journal of Environmental Economics and Management, 38(1): 20-48.

Alberini, Anna, and Shelby Frost. 2007. “Forcing Firms to Think About the Future: Economic Incentives and the Fate of Hazardous Waste.” Environmental & Resource Economics, 36(4): 451–474.

Alberini, Anna, et al. 2005. “The role of liability, regulation and economic incentives in brownfield remediation and redevelopment: Evidence from surveys of developers.” Regional Science and Urban Economics, 35(4): 327-351.

Alderson, David and Kevin Soo Hoo. 2004. “The Role of Economic Incentives in Securing Cyberspace.” Center for International Security and Cooperation (CISAC) Report, Stanford.

Armstrong and Sappington. 2007. “Recent Developments in the Theory of Regulation.” Handbook of Industrial Organization. Volume 3.

Arora, Seema, and Timothy N. Cason. 1996. “Why Do Firms Volunteer to Exceed Environmental Regulations? Understanding Participation in EPA's 33/50 Program.” Land Economics, 72(4): 413-432.

Attanasio, Meghir, and Santiago. 2011. “Education Choices in Mexico: Using a Structural Model and a Randomized Experiment to Evaluate PROGRESA.” The Review of Economic Studies. Volume 79: 37-66.

Auerbach, A.J. and K.A. Hassett (1991), “Recent U.S. investment behavior and the Tax Reform Act of 1986: a disaggregate view,” Carnegie-Rochester Conference Series on Public Policy 35:185-215.

Aurora, Ashish, Ramayya Krishnan, Rahul Telang, and Yubao Yang. 2009. “An Empirical Analysis of Software Vendors’ Patch Release Behavior: Impact of Vulnerability Disclosure.” Information Systems Research, 21(1): 115–132.

Baily, M., and R. Lawrence, (1992), “Tax incentives for R&D: what do the data tell us?” Study commissioned by the Council on Research and Technology, Washington, DC.

Bakshi and Gans. 2009. “Securing the Containerized Supply Chain: Analysis of Government Incentives for Private Investment.” Management Science. Volume 56: 219-233.

Banerjee, Abhijit, and Barry D. Solomon. 2003. “Eco-labeling for energy efficiency and sustainability: a meta-evaluation of US Programs.” Energy Policy, 31(2): 109-123.

Barnett, S.A. and P. Sakellaris (1998), “Nonlinear response of firm investment to Q: testing a model of convex and nonconvex adjustment costs,” Journal of Monetary Economics (October 1998):261-288.

Bennear, Lori S., and Shelia M. Olmstead. 2008. “The impacts of the "right to know”: Information disclosure and the violation of drinking water standards.” Journal of Environmental Economics and Management, 56(2): 177-130.

Bernanke, B., H. Bohn, and P. Reiss, (1988), “Alternative non-nested specification tests of time series investment models.” Journal of Econometrics, 37(2):293–326.

Bisogni, Fabio, Simona Cavallini, and Sara di Trocchio. “Cybersecurity at European Level: The Role of Information Availability.” Communications & Strategies, 81: 105-124.

Blackman, Allen, Sarah Darley, Thomas P. Lyon, and Kris Wernstedt. 2010. “What Drives Participation in State Voluntary Cleanup Programs? Evidence from Oregon.” Land Economics, 86 (4): 785-799.

Bloom, N., R. Griffith, and J. van Reenen, (2002) “Do R&D tax credits work? Evidence from a panel of countries 1979-1997.” Journal of Public Economics 85, 1-31.

Böhme, Rainer, and Galina Schwartz. 2010. “Modeling Cyber-Insurance: Towards A Unifying Framework.” Working paper presented at the Workshop on the Economics of Information Security, Harvard University.

Bolot, Jean, and Marc Lelarge. 2008. “Cyber Insurance as an Incentive for Internet Security.” Paper presented at the Workshop on the Economics of Information Security, Hanover, NH.

Branco, Manuel Castelo and Lúcia Lima Rodrigues. 2006. “Corporate Social Responsibility and Resource-Based Perspectives.” Journal of Business Ethics, 69(2): 111-132.

Brännlund, Runar, Sofia Lundberg, and Per-Olov Marklund. 2009. "Assessment of green public procurement as a policy tool: Cost-efficiency and competition considerations." Umea Economic Studies (Working Paper) No 775.

Brouhle, Keith, and Donna Ramirez Harrington. 2010. "GHG Registries: Participation and Performance Under the Canadian Voluntary Climate Challenge Program." Environmental and Resource Economics, 47 (4): 521-548.

Brown, Jeffrey R., and J. David Cummins, Christopher M. Lewis and Ran Wei. 2004. “An empirical analysis of the economic impact of federal terrorism reinsurance.” Journal of Monetary Economics, 51: 861-898.

Bryden, Anna, et al. 2013. “Voluntary agreements between government and business—A scoping review of the literature with specific reference to the Public Health Responsibility Deal.” Health Policy, 110(2-3): 186-197.

Burby, Raymond J. 2006. “Hurricane Katrina and the Paradoxes of Government Disaster Policy: Bringing About Wise Governmental Decisions for Hazardous Areas.” The ANNALS of the American Academy of Political and Social Science, 604: 171-191.

Caballero, R.J., E.M.R.A. Engel and J.C. Haltiwanger (1995), “Plant-level adjustment and aggregate investment dynamics,” Brookings Papers on Economic Activity 2:1-54.

Cambini, Carlo, and Laura Rondi. 2010. “Incentive regulation and investment: evidence from European energy utilities.” Journal of Regulatory Economics, 38(1): 1-26.

Cantwell, J. and R. Mudambi, (2000), “The location of MNE R&D activity: The role of investment incentives,” 40 Management International Revue, 127.

Chatterji, Aaron K., and Michael W. Toffel. 2010. “How Firms Respond to Being Rated” Strategic Management Journal, 31(9): 917-945.

Chatterji, Aaron K., Kenneth Y. Chay, and Robert W. Fairlie. 2013. “The Impact of City Contracting Set-Asides on Black Self-Employment and Employment.” Forthcoming in Journal of Labor Economics.

Chirinko, R.S., S. M. Fazzari, and A.P. Meyer, (1999), “How responsive is business capital formation to its user cost?: An exploration with micro data.” Journal of Public Economics, 74(1):53–80.

Cohen, D. and J. Cummins (2006), “A Retrospective Evaluation of the Effects of Temporary Partial Expensing,” Finance and Economics Discussion Series #2006-19, Divisions of Research and Statistics and Monetary Affairs, federal Reserve Board, Washington D.C.

Cordes, J. 2011. An Overview of the Economics of Cybersecurity and Cybersecurity Policy. George Washington University Cybersecurity Policy and Research Institute. Report GW-CSPRI-2011-6.

Cummins, J.G., K.A. Hassett and R.G. Hubbard (1994), "A reconsideration of investment behavior using tax reforms as natural experiments," Brookings Papers on Economic Activity 2:1-74.

Cummins, J.G., K.A. Hassett and R.G. Hubbard (1996), "Tax reforms and investment: a cross-country comparison," Journal of Public Economics 62:237-273.

Cyber Data Risk Managers. 2013. 2013 Data Privacy, Information Security and Cyber Insurance Trends.

Dalen, Dag Morten, Espen R. Moen, and Christian Riis. 2006. "Contract renewal and incentives in public procurement." International Journal of Industrial Organization, 24: 269-285.

Dalley, Paula J. 2007. "The Use and Misuse of Disclosure as a Regulatory System." Florida State University Law Review, 34(4): 1089–1131.

Delmas, Magali, Maria J. Montes-Sancho, and Jay P. Shimshack. 2010. "Information Disclosures Policies: Evidence from the Electricity Industry." Economic Inquiry, 48(2): 483-498.

Department of Homeland Security. 2012. Cybersecurity Insurance Workshop Readout Report.

Desai, M.A. and A.D. Goolsbee, (2004), "Investment, Overhang, and Tax Policy," Brookings Papers on Economic Activity, no. 2 (Fall 2004), 275-328.

Dourado, E. 2012. Internet Security without Law: How Service Providers Create Order Online. Mercatus Center at George Mason University. Working Paper No. 12-19

Dourado, E., and Brito, J. 2012. Is There a Market Failure in Cybersecurity? Mercatus Center at George Mason University. Mercatus on Policy No. 106.

Dynes, Scott, Eric Goetz, and Michael Freeman. 2008. "Cybersecurity: Are Economic Incentives Adequate?" IFIP International Federation for Information Processing, 253: 15-27.

Edgerton, J., (2010), "Investment incentives and corporate tax asymmetries," Journal of Public Economics, 94 (December 2010), 936-952.

Eeten, M. and Bauer, J. 2008. Economics of Malware: Security Decisions, Incentives and Externalities. Organisation for Economic Co-operation and Development (OECD), Directorate for Science, Technology, and Industry (STI). STI Working Paper 2008/1

Égert, Balázs. 2009. "Infrastructure Investment in Network Industries: The Role of Incentive Regulation and Regulatory Independence." CESifo (Center for Economic Studies and Ifo Institute for Economic Research) working paper, No. 2642.

Eisner, R., (1969), "Tax policy and investment behavior: comment." American Economic Review, 59(3): 379–388.

Etzioni, A. Fall 2011. Cybersecurity in the Private Sector. Issues in Science and Technology, pp. 58-62.

Fiszbein, et. al. 2009. "Conditional Cash Transfers: Reducing Present and Future Poverty." World Bank.

Gal-Or, Esther, and Anindya Ghose. 2005. "The Economic Incentives for Sharing Security Information." Information Systems Research, 16(2): 186-208.

Goetz, Kimberly S. 2010. “Encouraging sustainable business practices using incentives: a practitioner's view.” Management Research Review, 33(11): 1042-1053.

Goolsbee, A.D. (2000), “Taxes and the quality of capital,” Mimeograph (University of Chicago).

Goolsbee, A.D., (1998a), “Does government R&D policy mainly benefit scientists and engineers? 88 American Economic Revue, 298.

Goolsbee, A.D., (1998b), “Investment tax incentives and the price of capital goods,” Quarterly Journal of Economics, 113:121-148.

Gordon, L. A. and M. P. Loeb, Managing Cybersecurity Resources: A Cost-Benefit Analysis (McGraw-Hill, Inc.), 2006.

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn. 2003. “Sharing Information on Computer Systems Security: An Economic Analysis.” Journal of Accounting and Public Policy, 22(6): 461-485.

Graetz, M. and R. Doud, (2012), “Technological innovation, international competition, and the challenges of international income taxation.” Columbia Law Review, 113, 347-446.

Graham, Mary, and Catherine Miller. 2001. “Disclosure of Toxics Releases in the United States.” Environment: Science and Policy for Sustainable Development, 43(8): 8–20.

Greene, Mark R. 1979. “A Review and Evaluation of Selected Government Programs to Handle Risk.” Annals of the American Academy of Political and Social Science, 443: 129-144.

Griffith, R., D. Sandler, and J. van Reenen, (1995), “Tax incentives for R&D,” Fiscal Studies 16 (2), 21–44.

Griffith, R., S. Redding, and J. van Reenen, (2001), “Measuring the cost effectiveness of an R&D tax credit for the UK,” 22 Fiscal Studies, 375.

Gugerty, Mary Kay. 2009. “Signaling Virtue: Voluntary Accountability Programs among Nonprofit Organizations.” Science Policy, 42(3): 243-273.

Hahn, Robert W., and Anne Layne-Farrar. 2006. “The Law and Economics of Software Security.” Harvard Journal of Law and Public Policy, 30(1): 283-353.

Hall, B., (1993), “R&D tax policy during the 1980s: success or failure?” in Poterba, J., ed., Tax Policy, and the Economy, 29, 1–35.

Hassett, K.A. and R.G. Hubbard (1998), “Are investment incentives blunted by changes in the price of capital goods?” International Finance 1:103-126.

Hassett, K.A. and R.G. Hubbard, (2002), “Tax policy and business investment,” in Auerbach A. and M. Feldstein, Handbook of Public Economics (Elsevier, Amsterdam).

Hausken, Kjell. 2006. “Income, interdependence, and substitution effects affecting incentives for security investments.” Journal of Accounting and Public Policy, 25(6): 629-665.

Hausken, Kjell. 2007. “Information sharing among firms and cyber attacks.” Journal of Accounting and Public Policy, 26(6): 639-688.

Hines, J. and A. Jaffe, (2000), “International taxation and the location of inventive activity,” in Hines, J.R., ed., International Taxation and Multinational Activity 201.

Hines, J., (1994). “No place like home: tax incentives and the location of R&D by American multinationals.” Tax Policy and the Economy 8, 65–104.

Hines, J., (1998). “Is it investment ramifications of distortionary tax subsidies.” Working Paper 6615 (National Bureau of Economic Research).

House, C. and M. Shapiro (2008), “Temporary Investment Tax Incentives: Theory with Evidence from Bonus Depreciation,” American Economic Review 98 No. 3 (June, 2008): 737- 768.

Jaffee, Dwight M., and Thomas Russell. 1997. “Catastrophe Insurance, Capital Markets, and Uninsurable Risks.” The Journal of Risk and Insurance, 64(2): 205-230.

Jin, Ginger Zhe, and Phillip Leslie. 2003. “The Effect of Information on Product Quality: Evidence from Restaurant Hygiene Grade Cards.” The Quarterly Journal of Economics, 118(2): 409-451.

Jin, Ginger Zhe, and Phillip Leslie. 2009. “Reputational Incentives for Restaurant Hygiene.” American Economic Journal: Microeconomics, 1(1): 237-267.

Johnston, Jason Scott. 2005. “The Promise and Limits of Voluntary Management-Based Regulatory Reform: An Analysis of EPA's Strategic Goals Program.” U of Penn, Inst for Law & Econ Research Paper No. 05-17; U of Penn Law School, Public Law Working Paper No. 06-05.

Joskow, Paul. 2013. “Incentive Regulation in Theory and Practice: Electricity Distribution and Transmission Networks.”

Karamanos, Panagiotis. 1999. “Voluntary environmental agreements for the reduction of greenhouse gas emissions: Incentives and characteristics of electric utility participants in the climate challenge program.” Dissertations and Theses; Thesis (Ph.D.)--Indiana University.

Khanna, Madhu, and William Rose Q. Anton. 2002. “Corporate Environmental Management: Regulatory and Market-Based Incentives.” Land Economics, 78(4): 539-558.

Khanna, Madhu, Patricia Koss, Cody Jones, and David Ervin. 2007. “Motivations for Voluntary Environmental Management.” Policy Studies Journal, 35(4): 751–772.

Khanna, Madhu, Wilma Rose H. Quimio, and Dora Bojilova. 1998. “Toxics Release Information: A Policy Tool for Environmental Protection.” Journal of Environmental Economics and Management, 36(3): 243–266.

Knittel, M. (2007), “Corporate Response to Accelerated Tax Depreciation: Bonus Depreciation for Tax Years 2002-2004,” Office of Tax Analysis Working Paper 98, U.S. Department of the Treasury.

Kobayashi, B. 2011. An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods. George Mason University School of Law, Law and Economics Working Paper Series.

Kobayashi, Bruce H. 2005. “An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and Other Public Security Goods.” Law and Economics Working Paper Series.

Konar, Shameek, and Mark A. Cohen. 1997. “Information as Regulation: The Effect of Community Right to Know laws on Toxic Emissions.” Journal of Environmental Economics and Management, 32(1): 109–124.

Krasnokutskaya, Elena, and Katja Seim. 2011. “Bid Preference Programs and Participation in Highway Procurement Auctions.” The American Economic Review, 101(6): 2653-2686

Kremer and Williams. 2010. “Incentivizing Innovation: Adding to the Tool Kit.” Innovation Policy and the Economy. Volume 10

Kunreuther, Howard C., Mark V. Pauly, and Stacey McMorrow. 2013. Insurance and Behavioral Economics: Improving Decisions in the Most Misunderstood Industry. New York, NY: Cambridge University Press.

Kunreuther, Howard. 2002. "The role of insurance in managing extreme events: Implications for terrorism coverage." Business Economics, 37(2): 6-16.

Kunreuther, Howard. 2008. "Reducing Losses from Catastrophic Risks through Long-Term Insurance and Mitigation." Social Research, 75(3): 905-930, 1033.

Laffont, Jean-Jaques and Jean Tirole. 1993. A Theory of Incentives in Procurement and Regulation, Massachusetts Institute of Technology Press.

Landry, Craig E., and Jingyuan Li. 2012. "Participation in the Community Rating System of NFIP: Empirical Analysis of North Carolina Counties." Natural Hazards Review, 13(3): 205–220.

Lelarge, M., and Bolot, J. 2009. Economic Incentives to Increase Security in the Internet: The Case for Insurance. IEEE INFOCOM 2009 proceedings.

Lelarge, Marc, and Jean Bolot. 2009. "Economic Incentives to Increase Security in the Internet: The Case for Insurance." INFOCOM 2009, IEEE. 1494-1502.

Lesk, M. November/December 2011. Cybersecurity and Economics. IEEE Security & Privacy.

Lychagin, S. et al., (2010), "Spillovers in space: does geography matter?" Center For Economic Performance, Discussion Paper No. 991.

Machin S. and J. van Reenen, (1998), "Technology and changes in skill structure: Evidence from seven OECD countries," 113 Quarterly Journal of Economics, 1215.

Mamuneas, T., and M. Nadiri, (1996), "Public R&D policies and cost behaviour of the U.S. manufacturing industries." Journal of Public Economics 63, 57–81.

Mansfield, E., (1986). "The R&D tax credit and other technology policy issues." American Economic Association Papers and Proceedings 76, 190–194.

Mazurek, Janice. 2002. "Government-sponsored voluntary programs for firms: An initial survey." New Tools for Environmental Protection: Education, Information, and Voluntary Measures. The National Academies Press, National Academy of Sciences: 219-234.

McCutchen, W.W. Jr. (1993), "Estimating the impact of the R&D tax credit on strategic groups in the pharmaceutical industry, 22 Res. Policy, 337.

Michel-Kerjan, Erwann, and Paul Raschky. 2011. "The Effects of Government Intervention on The Market for Corporate Terrorism Insurance." University of Pennsylvania, Wharton School working paper # 2011-05.

Miller, Steven R., Abdul O. Abdulkadri, Sandra S. Batie, and Satish V. Joshi. 2012. "Motivation, Barriers and Incentives for the Participation of Livestock Operations in MAEAP." Dept. of Agricultural, Food, and Resource Economics Staff Paper Series.

Moon, Seong-gin. 2008. "Corporate Environmental Behaviors in Voluntary Programs: Does Timing Matter?" Social Science Quarterly, 89(5): 1102–1120.

Moore, T. 2010. Introducing the Economics of Cybersecurity: Principles and Policy Options. Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy. pp. 3-23. National Research Council.

Moore, Tyler, and Richard Clayton. 2011. “The Impact of Public Information on Phishing Attack and Defense.” Communications & Strategies, 81: 45-68.

Moore, Tyler. 2010. “The economics of cybersecurity: Principles and policy options.” International Journal of Critical Infrastructure Protection, 3(3-4): 103-117.

Mulgan, et. al., 2011. “Social Impact Investment: the challenge and opportunity of Social Impact Bonds.” The Young Foundation

Mulligan, Deirdre K., and Fred B. Schneider. 2011. “Doctrine for Cybersecurity.” Daedalus, 140(4): 70-92.

Myers, Samuel L., and Tsze Chan. 1996. “Who Benefits from Minority Business Set-Asides? The Case of New Jersey.” Journal of Policy Analysis and Management, 15(2): 202-226.

Plummer, E., (2000), “Incentive effects of the investment tax credit: Evidence from analysts' forecasts,” in (ed.) 12 (Advances in Taxation, Volume 12), Emerald Group Publishing Limited, 127-171.

Post, Joseph, Michael Wells, James Bonn, and Patrick Ramsey. 2011. “Financial Incentives for NextGen Avionics.” Ninth USA/Europe Air Traffic Management Research and Development Seminar.

Rao, N. (2013), “Do tax credits stimulate R&D spending? The effect of the R&D tax credit in its first decade,” (The Wagner School, New York University).

Rue, R., and Pfleeger, L. July/August 2009. Making the Best Use of Cybersecurity Economic Models. IEEE Security & Privacy.

Sappington, David E. 2003. “The Effects of Incentive Regulation on Retail Telephone Service Quality in the United States.” Review of Network Economics. Volume 2, Issue 4: 355-375.

Sappington, David E. M., and Dennis L. Weisman. 1994. “Designing superior incentive regulation: Accounting for all.” Fortnighty, 132(4): 12-15.

Segerson, Kathleen ed. 2002. Economics and Liability for Environmental Problems. Aldershot, UK and Burlington, VT: Ashgate Publishing Co.

Segerson, Kathleen, and Thomas J. Miceli. 1998. “Voluntary Environmental Agreements: Good or Bad News for Environmental Protection?” Journal of Environmental Economics and Management, 36(2): 109-130.

Segerson, Kathleen. 2006. “Chapter 10: An Assessment of Legal Liability as a Market-Based Instrument” in Moving to Markets in Environmental Regulation: Lessons from Twenty Years of Experience. Oxford Scholarship Online.

Shapiro & Rabinowitz. “Voluntary Regulatory Compliance in Theory and Practice: The Case of OSHA.” Administrative Law Review Volume 52: 97-155.

Shetty, Nikhil, Galina Schwartz, Mark Felegyhazi, and Jean Walrand. 2010. “Competitive Cyber-Insurance and Internet Security.” Economics of Information Security and Privacy, 229-247.

Simon, Paul, et al. 2005. “Impact of Restaurant Hygiene Grade Cards on Foodborne-Disease Hospitalizations in Los Angeles County.” Journal of Environmental Health, 67(7): 32–36.

Stahl, Michael M. 1994. “Promoting Voluntary Compliance: A Valuable Supplement to Environmental Enforcement.”

Summers, L., (1981), “Taxation and corporate investment: A Q-theory approach.” Brookings Papers on Economic Activity, 1:67–140.

Thomson, R. and Jensen, J. (2011), “The Effects of public subsidies on R&D employment, evidence from OECD Countries, (Intellectual Property Research Institute of Australia, Working Paper No. 2/11).

U.S. Department of Commerce, Internet Policy Task Force, "Cybersecurity, Innovation, and the Internet Economy" (Green Paper), June 2011

U.S. Department of Homeland Security, Cross Sector Cyber Security Working Group, Incentives Subgroup. September 2009. Incentives Recommendations Report.

U.S. Department of Homeland Security. November 2012. Cybersecurity Insurance Workshop Readout Report.

U.S. Government Accountability Office, (1989), “Tax policy and administration: The research tax credit has stimulated some additional research spending.”

U.S. House of Representatives, House Republican Cybersecurity Task Force. October 2011. Recommendations of the House Republican Cybersecurity Task Force.

U.S. National Research Council. 2010. Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy.

Verma, Kiran, Barry M. Mitnick, and Alfred A. Marcus, 1999. “Making Incentive Systems Work: Incentive Regulation in the Nuclear Power Industry.” Journal of Public Administration Research and Theory: J-PART, 9(3): 395-436.

Videras, Julio, and Anna Alberini. 2000. “The appeal of voluntary environmental programs: which firms participate and why?” Contemporary Economic Policy, 18(4): 449-460.

Vogelsang, Ingo. 2002. “Incentive Regulation and Competition in Public Utility Markets: A 20-Year Perspective.” Journal of Regulatory Economics. Volume 22: 5-27.

Weil, David, Archon Fung, Mary, Graham, and Elena Fagotto. 2006. “The Effectiveness of Regulatory Disclosure Policies.” Journal of Policy Analysis and Management, 25(1): 155-181.

Wernstedt, Kris, Peter B. Meyer, and Anna Alberini. 2006. “Attracting Private Investment to Contaminated Properties: The Value of Public Interventions.” Journal of Policy Analysis and Management, 25(2): 347-369.

White House. n.d. “Cyber-Insurance Metrics and Impact on Cyber-Security.” Undated policy white paper. Accessed April 25, 2013.

Wilson, Daniel J., (2009), “Beggar thy neighbor? The in-state, out-of-state, and aggregate effects of R&D tax credits,” 91 Revue of Economics and Statistics, 431.

Yusof, Nor’Aini, Ismael Younis Abu-Jarad, and Mohd Hasanal Badree. 2012. “The Effectiveness of Government Incentives to Facilitate an Innovative Housing Delivery System: The Perspective of Housing Developers.” Theoretical and Empirical Researches, 7(1): 55-68.

Zhang, Yichen. 2009. “Incentives for Poultry Integrators to Contract Bio-Secure Producers and Implication for Government Indemnification Program.” Master’s Thesis, Mississippi State University, Department of Agricultural Economics.

3.3. DHS Incentives Workshop Summary

Incentives Working Group

Workshop Notes

Date: April 19, 2013

Location: 1110 N. Glebe Road, Arlington, VA 22201, Executive Briefing Facility

In addition to the panelists listed below, participants in the workshop included the following Federal Government departments and agencies: Department of Agriculture, Department of Commerce, Department of Defense, Department of Education, Department of Energy, Department of Health and Human Services, Department of Homeland Security, Department of State, Department of Transportation, Department of the Treasury, Environmental Protection Agency, Federal Communications Commission, Federal Deposit Insurance Corporation, Food and Drug Administration, General Services Administration, National Guideline Clearinghouse, National Institute of Standards and Technology, National Security Staff, and the Office of the Director of National Intelligence.

Industry and nongovernmental participants included representatives from AIG, American Fuel and Petrochemical Manufacturers, American Gas Association, American Public Power Association, Association of Metropolitan Water Agencies, BNY Mellon, Boeing, Booz Allen Hamilton, CSC, Deloitte, Dickstein Shapiro, Fire Eye, General Dynamics, General Electric, Homeland Security Studies and Analysis Institute, Information Technology & Innovation Foundation, International Legal Technology Association, Internet Security Alliance, Juniper Networks, Lockheed Martin, LSB Industries, National Association of Regulatory Utility Commissioners, National Defense Industrial Association, NERC, Northrup Grumman, Praxair, Sacramento Municipal Utility District, SAIC, Securities Industry and Financial Markets Association, U.S. Chamber of Commerce, USAA, Utilities Telecom Council, Verizon, and Worldwide Insight.

3.3.1. Welcome and Agenda Overview

Bob Kolasky described ITF's role. It is important that the work on incentives is done well and transparently. A principle goal is including perspective of critical infrastructure community.

3.3.2. Keynote 1

Acting Deputy Under Secretary McConnell began with recognition of the tragic Boston bombings. He noted that there is, today, a strategic moment for cybersecurity; we are lucky that there has not yet been a loss of life due to cyber attacks, but that likely is coming. Today, we are putting in place part of a larger effort to create a partnership to stop the growth of these problems. We are here to explore the art of the possible with respect to what the public-private partnership can be and can achieve.

There is significant interconnection between cybersecurity and infrastructure. PPD 21 has a broader focus than just protection, and takes a holistic and strategic view of things. There are three key elements to the EO: (1) privacy and civil liberties and rights, (2) information sharing, and (3) Cybersecurity Framework. This will be a voluntary Framework, and no other aspects of the Executive Order (EO) rely on adoption of the Framework.

The Framework will be the result of the extensive and collaborative effort conducted by the National Institute of Standards and Technology (NIST). The Framework will reference technical controls, but it will be more than that. It will be a risk management Framework, including resilience and not just focused on protection. The Framework will not only be for the technical community, but will be brought to corporate boards and leadership. It will have words understandable to such audiences, and include potential investments that need to be made within a risk management Framework.

The Framework is due by mid-February 2014, and will allow stakeholders tell DHS if they will utilize the voluntary program.

PS-Prep is one example of a voluntary incentive program. Though three organizations (AT&T, the American Bar Association, and RASGAS) are now certified, this is not a resounding uptake (later in the workshop it was noted that a fourth organization has recently completed its conformity assessment and will be eligible to receive its certification soon). So it seems that PS-Prep is not using the right incentives. That is why we are holding this meeting. We want to know: how can we get it right? What are the right incentives? Currently, there is also fiscal restraint, making some incentives harder to institute than others. We may require many incentives, including regulations and legislation. But, we have a great set of people working on this.

3.3.3. Keynote 2

Larry Clinton, President and CEO of the Internet Security Alliance, began by noting that government and industry have aligned, but not identical security goals. Hope to fill in the gap today. Business interests reflect business requirements. We are thinking about cyber all wrong. It is not just a tech issue, but an enterprise issue. The problem is people, not technology. Just because you are breached, you (firms) are not necessarily negligent. There are two types of companies, those who know they were attacked and those who don't know. Perimeter defense is outmoded. This is not just like seatbelts; is not a consumer product safety issue. Systems are not bad, but they are under attack, and there are many incentives to attack them. It is not true that industry does not want to spend on cyber. Spending has doubled (from $40 to 80 billion) in recent years.

This is more than the $59B spent each year for all DHS. The notion of perimeter defense is a thing of the past, as it possible to defend systems even if you have been breached. Billions for eHealth records and standards in recent funding (stimulus, etc.); but, health sector is among worst – Johns Hopkins University study, PriceWaterhouseCoopers (PwC) study.

It is inappropriate to focus on regulation, as they are static, U.S.-specific, often set ceilings when we really need floors, don't necessarily work (can be bad for security as they may push too much focus on compliance – which can be anti-security), and hard to make work.

Incentives are as important to cybersecurity as is technology, but the incentives favor the attackers (cheap and easy to access, and normally one generation ahead of defenders, and few prosecutions), government and industry have different jobs and see "risk" differently (with the private sector often more risk tolerant than government), often the risk taker is not the damage sufferer, with irresistible incentives often promoting insecurity. For example, the cloud, modern supply chains, and other aspects of modern systems are inherently insecure and prevalent because they make business easier.

There are massive economic incentives to be insecure. People have been moving from traditional telephony to voice over Internet Protocol (VoIP); international supply chain; cloud computing –PwC study – 62% had little or no faith in cloud, including 48% that had already done that. Standards can lead to insecurity; suggest pen testing is reduced from quarterly to annually for compliance with the Framework.

There is a long and successful history of government/industry partnerships using economic incentives, e.g., the power grid and telephone network. However, if cyber is a big problem, a big deal is required. How should this be done?

Again, many sectors are involved here; thus, we may require a menu of incentives, even within sectors. In fact, incentives must apply at the corporate level, not the sector level.

A century ago – hot technology was power and phone – U.S. government guaranteed rate of return to utilities so that they would invest in less profitable, rural areas.

What are the goals of the Framework? Adopt the Framework (what is the Framework?), prevent catastrophic attacks (including acts of war, which would be a federal job), protect personally identifiable information (PII) or IP? Maybe best to incentivize innovation, but not compliance (can use large public sector players with economies of scale to assist smaller players)?

Acts of war are supposed to be prevented by national government, are private sector companies supposed to now? If so, 900% spending increase. Is program going to lead to greater security? Didn't with healthcare or federal Information Security Management Act (FISMA).

Incentives are best viewed through a series of principles, including that in order to be effective incentives must be: powerful enough to affect corporate investment behavior, calibrated to match the level of additional investment required to adopt the Framework, vary not just from sector to sector but business to business and thus a menu of incentives will be needed, recognize that regulation that does not include full cost recovery is not a substitute for incentives, and that cost not compensated through incentives will either be passed on to consumers or reduce investment in critical infrastructure - there is no free lunch to be had.

3.3.4. Session I: Regulated Industries

Session I featured five panelists from regulated industries: Anna Cochrane of the Federal Energy Regulatory Commission, Will Coffman of the American Public Power Association, Miles Keogh of the National Association of Regulatory Utility Commissioners, Jim Linn of the American Gas Association, and Karl Schimmeck of the Financial Services sector. Moderated by Rob Atkinson of the Information Technology and Innovation Foundation, questions from the first session included the following:

- What incentives are there to share information?
- Does cost recovery work as an incentive?
- Will the smart grid help utilities with cybersecurity?
- Is rate recovery enough of an incentive to adopt the Framework if it is deemed a prudent investment?

Rob Atkinson: One approach to handling cybersecurity is legislation. There is no cost to the government and appears to provide security. The other extreme, often supported by business is to subsidize private sector cybersecurity while also providing them the freedom to fashion their own security. But it's obvious that funding for subsidies is extremely unlikely. What is needed is a middle ground that changes behavior but doesn't cost too much.

Karl Schimmeck (Financial Services): The Financial Services (FS) Sector seeks to create trust in dealing with the problem of cybersecurity which it sees as a real threat to the industry. While FS already uses incentives, the sector wants to see others adopt incentives. We suggest using limited federal investment in the right places. It's uncertain whether the Framework will make us safer, so is the idea that the Framework is the right path a correct assumption? Because the Framework has not been developed, there is nothing to incentivize as yet.

There are two threats: a national threat and a threat to business. The goal should be to set the appropriate level of response to each. We need to also consider disincentives, for example, the current system allows hackers get away with their actions; this needs to be addressed. We need standardization and harmonization of the Framework with international rules. Finally, industry has a concern about regulatory backlash, that is, how to encourage sharing of information in the face of the fear that the government might then use to information to regulate the sharers.

Incentives: Use the limited available money to fund R&D and provide grants to ISACs; if a certain level of security is reached, then the owner/operator can received incentives from the Government; share information across

sectors, but protect the sharers from liability; and, accelerate security clearances for sharing of classified information.

Miles Keogh (NARUC): All regulation is some sort of incentive, either a carrot or a stick. The trick is assuring that an apparent incentive isn't actually a stick, i.e., an orange stick. While cybersecurity is a new issue for State Public Utility Commissions (PUCs) to weigh in overseeing utility investments, it is not too exotic in the sense that any investment must be seen to be prudent, or a prudent cybersecurity investment is a prudent investment. However, PUCs need to be educated in cybersecurity, so they can ask the right questions concerning investments and understand the responses. A utility needs to construct a strategy to determine what a PUC expects from a rate case and educate the PUC. A risk management approach to cybersecurity is preferable to regulation in that prudent investments are what we want from utilities and the PUC system looks at prudence. A utility can increase spending on cybersecurity but it must be certain that the investment yields an increase in security.

Resilience – the utilities and PUCs need to agree on what this means before they can share a common understanding of what an investment in resilience is for. The value of any investment needs to be shown. The question then is: how do you create value via an investment?

Anna Cochran (FERC): FERC has mandatory cybersecurity standards to assure the reliability of the grid. FERC rules allow rate increase and a reasonable rate of return. There is some increased flexibility where extraordinary cost is incurred by a utility, e.g., a surcharge might be allowed after a hurricane. This is not an incentive, but a means to recover costs beyond the operator's control.

Incentives: Congress provided incentives to encourage transmission facilities to increase reliability through increased recovery of costs of investment. Because companies recover costs in different ways, some may be stronger competitively or have higher levels of security. Accordingly, non-rate based incentives would be preferable.

Jim Linn (AGA): Expedite clearances? The Energy Sector has this already. Information sharing? This should be done already, too. However, disclosure of information could make a company a larger target. Sharing of information describing the means of a cyber-attack could expose info on the system and needs protection. An approach that singles out a company based on expertise could also make the company a target.

Will Coffman (American Public Power Association - APPA): For the Electricity Sector, which already is regulated through FERC, design the Framework to reflect the existing FERC cyber standards rather than penalizing a company for participating in the program. Good incentives for the Electricity Sector: encouraged information sharing; increased numbers of clearances to access classified information, and certification programs. Adherence to these might result in lower insurance premiums. Finally, encourage companies to pass on cyber information they receive by providing liability protection.

Question: what are the differences in the regulatory sphere vs. the non-regulated sphere?

Karl Schimmeck: Because FS is already held to standards, the Framework should include those standards that are being met. This would prevent them from potentially being regulated again, despite meeting standards. The Framework should go beyond standards, like providing liability protection for information sharing.

Miles Keogh: Regulation is necessary for utilities to assure reliability, so the Framework could provide pressure for utilities to use best practices. Going beyond compliance with standards might be a seen as a disincentive. However, this concern can be mitigated by PUCs recognizing prudent investments in cost recovery decisions.

Question: what incentives are there to share information?

Karl Schimmeck: many companies worry that regulators will misuse information provided voluntarily. Also, removing liability for information sharing would encourage the practice.

Miles Keogh: One would want to change the culture of utilities, e.g., by educating managers in cybersecurity, training employees, and replacing a check-box mentality with a systems approach. First figure out how to incentivize this behavioral change, then information sharing should be straight-forward.

Anna Cochran: Can a safe-harbor be created for information-sharers? There is a provision in the FERC rules for this.

Jim Linn: If shared information was divulged, it exposes a company's security positions.

Question: Would an EPA Energy Star approach work, i.e., would providing a seal of approval as a cyber-secure company be a factor that would attract investors?

Jim Linn: No. It is preferable not to raise a company's profile. Investors might be guided by a seal, but that's a lesser concern than the increased targeting. There is no competitive advance to the seal and, moreover, we would prefer to have all companies at the same level of security.

Karl Schimmeck: Here are two types of R&D efforts: fund universities or DHS Centers to develop advanced cybersecurity technology; and encourage companies to put leading edge technology into use, but provide liability protection in case the company is sued because the technology wasn't adequately tested.

Anna Cochran: Recovery of R&D and installation of advanced technology costs are recoverable to utilities.

Question: Does cost recovery work as an incentive?

Miles Keogh: A prudent investment in cybersecurity is recoverable from PUCs if it is a sound, risk-based mechanism. If the mechanism is prudent, it will be approved.

Audience: Voluntary consensus standards are best practices. These might be the basis of the Framework. The Framework might give companies an incentive to undertake adoption and certification. Do industries adhere to best practices?

Miles Keogh: Don't certify, but instead incentivize companies to adopt best practices as the goal.

Question: Will the Smart Grid help utilities with cybersecurity?

Miles Keogh: The Grid's greater connectivity will create vulnerabilities, but greater resilience and cyber capacity will also be created, which might improve security.

Larry Clinton: It is important not to equate resilience and security.

Question: Should a PUC be overruled if it doesn't treat cybersecurity expenditures as a priority for political reasons, such as consumer resistance to higher bills?

Miles Keogh: A prudent investment will be approved. Will compliance with the Framework be deemed a prudent investment? FERC has mandatory standards, which are defined as prudent investments. If the Framework is well designed, but badly implemented or doesn't lead to prudent decision-making, then expenditures won't be approved.

Question: Is rate recovery enough of an incentives to adopt the Framework, if it is deemed a prudent investment?

Miles Keogh: There might be other factors than rate recovery, e.g., economic considerations.

Jim Linn: The Gas Industry will be taking steps to assure cybersecurity in any case.

Caller (AIG): What is the value of a Framework if we don't understand the risk?

Panel summary: Three incentives: (1) liability protection for information sharing; (2) innovation creates risks, so protection is needed for innovation; and (3) improve R&D with liability protection.

3.3.5. Session II: Non-Regulated Industries

Session II reviewed incentives-related issues specific to non-regulated industries. Moderated by Roberta Stempfley of DHS, the panel included the Internet Security Alliance's Clinton, Brian Finch (Dickstein Shapiro LLP, a law firm that advises SAFETY Act applicants), Marc Sachs (Verizon), and John Toomer (Boeing). Questions from the second session included the following:

- What is the current environment in non-regulated sectors like from your viewpoint?
- Can other programs that rely on social behavior be adapted to incentivize the Framework?
- How about research and development tax credits accessible to regional clusters and patent protection as incentives?
- If the Framework had a risk-based approach, how would it work?

Question: What is the environment in non-regulated sectors from your viewpoint?

John Toomer (Boeing): Boeing has two components, the defense component that is part of the DIB and the commercial which is regulated. Cybersecurity is a given in all aspects of the business and in the companies that support Boeing. As a result, incentives won't affect us. Information sharing, however, is very important. The company wants to share best practices and has been doing so. Boeing is involved with eight sector ISACs. Cybersecurity is integral to the business and management is well aware of the issue and involved.

Boeing supports the Framework in general, but will wait so see what it looks like when developed. The Framework will need to address company suppliers which range from large to very small companies. There will need to be a variety of incentives for these.

Marc Sachs (Verizon): The Communications Sector has five components: wire, wireless, cable, broadcast, and satellite. Each is unique in that some have physical infrastructure, such as cables, while other deal more in the invisible aspects of communications. Some aspects of the industry are regulated.

The Communications Sector has three key elements: availability is critical to communications so there is a heavy emphasis to assure resilience; integrity must be there to assure that information is not compromised; and confidentiality is more of a customer issue, since they need to take steps if this is important, whereas the carrier simply delivers the information. The industry is highly targeted by cyber-attacks.

Brian Finch (Dickstein Shapiro LLP): Does the SAFETY Act apply to cyber-attacks? The Framework is just the latest exercise in partnership, starting with the NIPP, followed by PS-PREP. Just as those partnerships needed incentives, such as liability protection, to gain partners, so does the Framework. The SAFETY Act could provide this incentive. Consider that over 700 technologies have been approved by DHS under the Act. The Act establishes affirmative liability protection for users of approved technology if sued. The Act denies awarding of punitive damages, but, more importantly, certifies a presumption of non-liability to third parties. If a party certified against third-party liability sells the technology to another party, the purchaser is also immune under the Act. Any technology that has a security purpose is included under the broad scope of the Act.

Why hasn't the Act been used in the cases of cybersecurity technology? First, most people are unaware of its potential applicability because it has been used solely for physical security. Second, over the 10 years since 9/11, we've suffered terrorism fatigue, causing us to downplay the importance of terrorism attacks.

Is more than applying the Act to cybersecurity needed? Perhaps, change phrasing so that the Act applies to more than "acts of terrorism," and that it applies to cyber terrorism and cyber technology. Because the Secretary of DHS makes determinations under the Act, these changes should be easy to make.

Larry Clinton (ISA): Do companies want subsidies? No, this is not an incentive. They understand the government's fiscal constraints and the need for pragmatism. If a program has value, it will be adopted. The Framework is too fuzzy right now. Industry has spent considerable sums on cybersecurity already and understands value. But does more need to be done? The Framework needs to get business to do more.

We don't know what the Framework will look like, but it should include language about risk-management. Also, it should address probabilities, consequences, and economics to make sense to business. Because senior managers are not savvy about digital information, taking cybersecurity out of the IT realm and putting it into the enterprise risk management realm will improve their understanding.

The Framework seems aimed at rudimentary attacks. Since attackers try this first, then raise the sophistication of the attack if this fails, the Framework needs to address progressive response to attacks. Also, consider cascading attacks, since not just one business is attacked, but connected businesses, both large and small, too. The Framework needs to cascade its protections down to these, too.

Question: Can other programs that rely on social behavior be adapted to incentivize the Framework?

John Toomer: There are large and small players, so recognize information sharing among large businesses for their benefit and then use the government to push out the information to the small businesses or create products for small businesses for adoption via incentives.

Over-compliance caused by duplicative federal, state, local agency, and customer audits of compliance result in duplication and diverting resources from cybersecurity. Create a central compliance audit to streamline the audit process to one audit. A good performer could be excused from follow-on audits.

Brian Finch: Amend the SAFETY Act to allow certification of international standards and practices that have proven effective. Since effectiveness is a sliding scale, create a sliding scale of incentives.

Marc Sachs: Industry needs assurance that liability from customer suits will be avoided if they take protective actions. If DHS wants industry to abandon what it is now doing under National Institute of Standards and Technology (NIST) standards to undertake the Framework, incentives will be needed. Because cyber-attacks do not respect political boundaries, if DHS wants businesses to adopt the Framework and come under federal oversight, then preempt states and localities.

From a financial perspective, tax credits and R&D provide too little incentive, but litigation and audits are very expensive and incentives in these areas would be attractive to large businesses.

Unknown party: The FTC (FCC?) rules of conduct to protect against botnets contain an appendix that details the barriers to adoption of the code of conduct and ways to circumvent the barriers that might be useful to the Framework incentives effort.

John Toomer: We want incentives for innovator companies. The threat is evolving, so we want protections to evolve, too. One approach would be an open innovation forum where ideas could be shared without fear of barriers and penalties. The government should encourage rather than inhibit this type of openness in order to engender trust and encourage those highly motivated enterprises.

Brian Finch: We have a cyber-problem, but who will benefit if the Framework is established? Probably not the large businesses. Figure out how to structure the Framework to get the best results. Litigation is very expensive. The SAFETY Act covers reasonable behavior if government-approved processes were used, as evidence of reasonable behavior.

Question: How about R&D tax credits accessible to regional clusters and patent protection as incentives?

Marc Sachs: For the Communications Sector, innovation is made by integration, processes, and systems rather than by things, so patent issues aren't applicable here.

Rob Yellen (AIG): Create incentives around enterprise risk management.

Larry Clinton: You need a menu of innovations for small companies, too.

John Toomer: Boeing has a number of small companies who aren't integrated into the general business so that they can be agile. Accelerating and streamlining patents would be helpful.

Brian Finch: Tax credits won't work. R&D and innovation work now without incentives, that is, new products have no problem enticing investors and customers. Instead, give resources for R&D and innovation through DHS centers and other entities. Maybe, large companies can get procurement advantage with government if they assist smaller companies with cybersecurity.

Larry Clinton: The government does many other things than allow tax incentives that should be explored.

Question: What definition of cyber incident should be used to trigger the SAFETY Act?

Brian Finch: Not sure, but it should be as broad as the definition of a terrorism incident under the Act. The definition should not be narrowed so that supply chain security involving compromised parts would be covered. Perhaps, "any damaging electronic attack" is about right

Question: If the Framework had a risk-based approach, how would it work?

Marc Sachs: What does "risk" mean? The Executive Order is based on consequence only. This is an important distinction and needs to be discussed in the EO context.

Larry Clinton: Risk means something different to government than to business. The government view of risk will not build partnership unless it recognizes business's concerns, such as economics.

John Toomer: It's all about brand, so that customers will want to use your products. Reputation is important in considering risk, but there is an economic component, too. The government needs to understand what business does.

Brian Finch: How bad will losses from stolen intellectual property and trade secrets be? This needs to be explored. More needs to be done to protect this investment.

3.3.6. Session III: Cross-Sector Incentives

Session III's Cross-sector Incentives panelists answered questions about their views on creating a competitive advantage for organizations seen as good stewards of cybersecurity, as well as how the Framework should address "signature-less" attacks. This panel was moderated by Bob Kolasky (DHS) and included Kevin Bonnette (SAIC), Tom Finan (DHS), Emile Monette (Government Services Administration), Don Perkins (Northrop Grumman), and Christine Ricci (General Electric).

Kevin Bonnette (SAIC): SAIC is prepared to embrace the Cybersecurity Framework and assist its clients with solutions to implement the Framework as well. Consider the shrinking budgets for the government and private

industry in reviewing the regulations and requirements each organization is expected to follow. The challenge going forward will be to understand the cost involved to meet expectations within the Framework.

Tom Finan (DHS): Mr. Finan supports Strategy and Policy within the Office of the Assistant Secretary for Infrastructure Protection National Protection and Programs Directorate (NPPD/IP). NPPD/IP is in a unique position to provide impact on the cybersecurity market. While DHS cannot offer a solution to fix everything, it is likely an organization to start the discussion between industry and the government.

Emile Monette (GSA): General Services Administration (GSA) has a Joint Working Group on Improving Cybersecurity and Resilience through Acquisition. The primary focus of the WG is Executive Order 13636 section 8(e), which requires a report on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. WG members include DHS, NIST, the Department of Defense, and the Office of Management and Budget (OMB). On April 25, a Request for Information (RFI) will be published in the federal Register. The RFI has three categories: feasibility, commercial practice, and steps that can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity. While the RFI will be left open for public comment for 30 days, GSA would prefer comments by May 15 so the feedback can be incorporated into the final document.

Don Perkins (Northrop Grumman): Northrop Grumman is currently dealing with the competition for risk security and rigor that comes through providing products and services. Like other organizations, it has developed practices through lessons learned. Ongoing dialogue between industry and government has also helped the organization create a multi-tiered approach to its incentives. Government should consider a similar multi-tied approach to pass along information. In addition, a lexicon to list common definitions and recognized standards would ensure that all who support cybersecurity are using the same terminology.

Private Sector Representative: Agreed with Mr. Perkins on the utility of a lexicon as there are individuals who do not understand what cybersecurity means. Similarly, some departments will define cybersecurity differently and it is important to have a similar understandings.

After the panelists provided an overview of their thoughts on cross-sector incentives, the following questions were posed to the group:

Question: In thinking about procurements, what are your thoughts about providing competing companies with a competitive advantage if their organization is seen as a good steward of cybersecurity?

Private Sector Representative: My primary concern with the approach would be within the details of the requirements. International companies will need to have enhanced levels of requirements. Additionally, several attendees of the workshop brought up ways this competitive advantage for companies could lead to disadvantages for the Federal Government. For example, it is unclear whether all the requirements can be measurable, which could lead to murky rulings that some businesses could deem unfair or the competitive advantage could largely favor big businesses that have the capital to meet all of the demands of the Framework.

Question: How will the recommendations harmonize with other existing requirements? Will it address "signature-less" attacks?

Kevin Bonnette: While correct in the need to harmonize the cybersecurity Framework with other existing requirements and legislation, it is important to note that this document is not expected to encompass everything for all departments and agencies. The Cybersecurity Framework will not be a one-size-fits-all recommendation.

Question: A private sector representative cautioned the Incentives Working Group on using the wording "secure product device" in lieu of calling a particular company secure. It is important the language dictate an understanding of the difference, because it will be possible to follow the Framework and not be secure.

Bob Kolasky: The Framework will be silent on a lot of these questions. At the moment, the definition for each incentive is being developed outside of the Framework.

3.3.7. Session IV: Government Roundtable

Session IV, the concluding Government roundtable, provided participants with an opportunity to hear from the Federal representatives responsible for drafting the incentives studies for their respective Government departments. It consisted of Tony Cheesebrough (DHS), Suzanne Lightman (Commerce Department, representing Ari Schwartz), and Leigh Williams (Treasury Department).

Tony Cheesebrough (DHS): Mr. Cheesebrough is the Chief Economist for the Integrated Task Force and the DHS National Protection and Programs Directorate. He provided an overview of the fourteen proposed incentives including the source documents from which each incentive was either recommended or discussed. For more information, review the slide deck titled "DHS Incentives Study: Objectives, Scope, Methodology, and Microeconomic Framework."

Emile Monette (GSA): GSA has a Joint Working Group on Improving Cybersecurity and Resilience through Acquisition. The primary focus of the WG is Executive Order 13636 section 8(e). Considering it is an interagency effort, WG members include DHS, NIST, DoD, and OMB.

On April 25, the Request for Information (RFI) will be published in the federal Register, visit http://www.regulations.gov. Submit comments via the federal eRulemaking portal by searching for "Notice-OERR-2013-01." Select the link "Submit a Comment" that corresponds with "Notice-OERR-2013-01." Follow the instructions provided at the "Submit a Comment" screen. Please include your name, company name (if any), and "Notice-OERR-2013-01" on your attached document by May 15.

Leigh Williams (Treasury): Treasury will review incentives based on four focus areas: (1) focus; (2) fair; (3) flexible; and (4) consistent. Treasury received some specific requirements within the EO to look at benefits and other items. Additionally, Treasury will want to ensure their work is integrated into the interagency deliverables appropriately.

Suzanne Lightman (NIST and Department of Commerce): Commerce will release a draft paper for public comment.

Question: How will incentives be analyzed?

Samara Moore: Incentives will be analyzed per the guidance in Section 9 of the EO, which addresses identifying cyber-dependent infrastructure.

Question: Will there be another look at incentives after the Framework is developed?

Tony Cheesebrough: We have received approval to amend our report based on feedback received during the incentives peer-review process, and so it is also possible that the incentives may be re-evaluated after the Framework is developed.

Question: What are some of the lessons from today's workshop that you will take back with you to your respective organizations?

Suzanne Lightman: Think carefully about how each incentive is defined and what ought to be considered an incentive.

Tony Cheesebrough: Liability protections were widely endorsed. Also, not only based on feedback today, but due to existing DHS efforts on expediting clearances as well as EO Section 4's requirements on information sharing, these two are not likely to be included in our recommendations.

Leigh Williams: Consider a multi-tiered approach to incentives.

3.4. Commerce NOI Response Review

On March 28, 2013, the Department of Commerce issued a 30-day Notice of Inquiry (NOI) entitled, "Incentives to Adopt Improved Cybersecurity Practices."[21] "Comments on Incentives to Adopt Improved Cybersecurity Practices NOI" were posted on April 29, 2013, and included 45 comments from the following respondents:[22]

Advanced Cybersecurity Center, American Association for Laboratory Accreditation, American Fuel and Petrochemical Manufacturers, American Gas Association, American Insurance Association, American Petroleum Institute, American Public Power Association, atsec, Booz Allen Hamilton, Bryan Rich, Business Software Alliance, CACI, Covington & Burling/Chertoff Group, DCS Corp, Donald Edwards, Dong Liu, Edison Electric Institute, Electric Power Supply Association, Emmanuel Adeniran, Encryptics, Federal Communications Commission, Financial Services Sector Coordinating Council, Gary Fresen, Honeywell, Internet Infrastructure Coalition, Internet Security Alliance, IT SCC, Los Angeles Department of Water and Power, Marsh, Microsoft, Monsanto, National Cable and Telecommunications Assoc., NCTA- The Rural Broadband Association, National Electrical Manufacturers Association, National Rural Electric Cooperative Association, Robin Ore, San Diego Gas & Electric and Southern California Gas Company, Sasha Romanosky, Southern California Edison, Telecommunications Industry Association, Terrence August & Tunay Tunca, U.S. Chamber of Commerce, US Telecom Association, Utilities Telecom Council, Voxem Inc.

As noted in Section 2.4.3, responses to the Commerce NOI were reviewed as a complement to the findings from the literature review, and to help inform conclusions about differences among evaluations as well as evaluations that are inconclusive. Similar to the DHS Incentives Workshop, the evaluation of NOI responses focused on the following questions:

- Are there additional incentive categories, or sub-categories, that should be considered?
- Which incentives are most likely and least likely to promote adoption of the voluntary Framework and why?

A summary of the 45 responses is provided below. Instead of a list detailing each response, a synopsis of responses is included for each category discussed in this report, as well as notable suggestions of particular interest. Additionally, Table 3 below indicates which of the incentives considered were recommended, discussed, or neither discussed nor recommended by each of the respondents.

[21] Docket number 130206115-3115-01: http://www.ntia.doc.gov/federal-register-notice/2013/notice-inquiry-incentives-adopt-improved-cybersecurity-practices
[22] The full responses can be accessed at: http://www.ntia.doc.gov/federal-register-notice/2013/comments-incentives-adopt-improved-cybersecurity-practices-noi

3.4.1. Grants

Respondents noted that significant costs could be associated with implementing the Cybersecurity Framework, depending on its final content and requirements. Several respondents suggested that grants could offset the investment required to implement new cybersecurity architecture, as well as to fund subsequent assessments to evaluate Framework adoption and associated impacts on system and network security. Respondents further noted the potential effectiveness of cross-sector grants to guide uniform maturity among critical-infrastructure owners and operators. For example, one respondent cited the potential for grant funds to enable information sharing and analysis centers to coordinate Framework adoption among member organizations, promoting economies of scale and minimizing the cost imposed on any individual entity. However, respondents also noted that the conditions for obtaining grants must not outweigh the estimated benefits from grant receipt.

3.4.2. Insurance, Liability Protections, and Legal Benefits

Numerous respondents suggested the potential value of various aspects of liability protection or a more robust cybersecurity insurance market. Notably, several respondents also mentioned a cybersecurity-specific SAFETY Act that could integrate several incentives to encourage Framework adoption and broaden cybersecurity investment. A common suggestion among respondents was the need for indemnity, at some level, from liability for security breaches if organizations adopting cybersecurity measures as defined in the Framework. Several respondents framed such indemnity as "safe-harbor protection", in which DHS or a third party would accredit an organization as making reasonable efforts to adopt the Framework, thereby triggering indemnity against certain legal claims. A respondent from the financial sector further noted that Framework adoption should entitle "protection from liability for FTC or State attorney general actions arising out of events or breaches relating to these practices, as such compliance constitutes sufficiently responsible and reasonable 'due care' behavior." However, other respondents noted that previous legislative attempts to codify some indemnity for adoption of cybersecurity best practices were insufficient to change the behavior of target organizations. Similarly, some respondents reported that a predictable process for validating Framework adoption is essential for the effectiveness of any indemnity regime, as organizations will require assurance that they are in fact covered under any such program before investing in Framework adoption. However, several respondents did note that the connection between a security breach and potential negligence may be fallacious in the current risk environment, as a highly adaptable threat implies that a certain number of breaches are inevitable regardless of cybersecurity measures.

Respondents further noted the potential importance of the cybersecurity insurance market to encourage adoption of appropriate security measures. The Cybersecurity Framework could provide a basis for a "standard of care" to support the issuance of cybersecurity insurance. As noted by one respondent, "cyber liability insurance represents both a financial incentive (i.e., protects an organization against loss, protects shareholder value) and a hidden penalty (i.e., over time insurance guidelines will establish higher standards of due care that will create costs for companies)" to encourage Framework adoption. A respondent also noted the relevance of the Terrorism Risk Insurance Act (TRIA) in providing coverage for losses attributable to a cybersecurity incident with a terrorism nexus, and the possibility of expanding TRIA criteria to encompass losses associated with other cyber malefactors.

Certain respondents also noted the application of the existing SAFETY Act in the context of Framework adoption. DHS does not believe, however, that is feasible without modifications to the Act.

3.4.3. Prioritized Technical Assistance

Several respondents noted the potential benefit of prioritized technical assessment for entities adopting the Cybersecurity Framework. Such assistance was suggested in three contexts: prioritized response from technical teams such as the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) after a

cybersecurity incident, preferred entry in cybersecurity training programs, and increased availability of vulnerability assessments, including on-site red-teaming and penetration testing. One respondent also suggested that DHS could assist adopters in securing priority Internet and telecommunications access during major incidents that result in service disruption.

3.4.4. Procurement Considerations

The potential benefits of incorporating Framework adoption into DHS or Federal procurement standards was suggested as a potentially low-cost, high-impact incentive. Respondents suggested that procurement considerations could allow the Framework to serve as a market differentiator, and increase the baseline cybersecurity of participants (a stated goal of the Framework). However, respondents also noted that procurement considerations would only affect the sub-set of critical infrastructure owners and operators that bid for Federal contracts. Furthermore, respondents emphasized that procurement considerations require a technology-neutral approach to cybersecurity, implying that such neutrality should be a foundational precept of the Framework if procurement is to be used as a viable incentive. This matches the Executive Order's requirement for the Framework to be technology-neutral.

3.4.5. Public Recognition

Public recognition was not frequently cited by respondents as a potentially effective incentive for encouraging adoption of the Framework. However, certain respondents did suggest existing recognition programs that could be applicable to Framework adoption. For example, a respondent noted that the Federal Government could establish a certification program to publicize that implementing entities have adopted the Framework, similar to the Payment Card Industry Data Security Standard certification. Another respondent noted the potential benefit of a "cybersecurity excellence" award in which participants could demonstrate their adherence to the Framework, which would then be evaluated by DHS or a third-party and could be reward by a qualifying moniker. A similar suggestion included authorizing certified organizations to use a particular image or logo on publicity materials to demonstrate the commitment of the awardee to cybersecurity.

3.4.6. Rate-Recovery for Price-Regulated Industries

The potential benefit of rate-recovery for cybersecurity costs for price-regulated industries was noted by several respondents. A common observation was the inability of price-regulated industries to invest in cybersecurity controls without the ability to pass on associated costs to a customer base. A utility trade association noted the potential effectiveness of directing the Federal Energy Regulatory Commission (FERC) to develop a cost recovery mechanism "allowing companies to go before the Commission to recover prudently incurred costs as a result of complying with federal cybersecurity mandate." Presumably such an approach could be used for other price-regulated industries, as well.

3.4.7. Security Disclosure

Mandated security disclosure was generally discussed by respondents as a disincentive for adopting the Framework. A respondent in the telecommunications sector noted: "The public disclosure of such attacks will do little – if anything – to compel such owners and operators to avoid security breaches, since they already have substantial incentives to do so. In fact, rather than act as an incentive, the public disclosure of such breaches would only serve to educate the attackers and increase the risk." Rather, respondents suggested that disclosure of security breaches should be encouraged as a voluntary best practice to promote information sharing on significant threats and vulnerabilities, but that barriers to disclosure such as potential liability should be resolved. Respondents further explained that breach disclosure, if encouraged or mandated, should be directly connected with a recommended cybersecurity mitigation to incentivize appropriate investment; otherwise such disclosures may be ineffective or encourage misallocation of resources.

3.4.8. Streamline Information Security Regulations

Respondents repeatedly cited inconsistent, overlapping, and duplicative information security regulations and guidelines as limiting standardized and measurably effective cybersecurity, and encouraged the government to reduce both the number and complexity of such requirements. A respondent suggested that owners and operators could be given credit for Framework adoption if they can demonstrate adopting similarly stringent standards recommended by their particular sector. Similarly, another respondent suggested a "Good Actor" benefit in which entities that pass an audit or review under one standard would be granted a time-defined exemption from similar reviews under duplicative regulations. Respondents also encouraged the preemption of state and local regulations, including privacy, tort, and contract laws that may impose obligations duplicating or conflicting with the Cybersecurity Framework. Respondents further suggested that the Framework should align existing regulations that artificially distinguish between sectors to ensure that entities providing functions across multiple sectors will be held accountable to a single standard.

3.4.9. Subsidies

Several respondents reported that costs are one of the most significant barriers to sufficient investment in effective cybersecurity, and that directing federal funding toward specific, Framework-compliant solutions could provide an incentive for Framework adoption. One respondent noted that "Federal subsidies and grants have been used successfully in other contexts in order to achieve important public policy goals when the conditions for obtaining such subsidies do not discourage their use, and their application in the cybersecurity environment could be appropriate." Notably, respondents did not differentiate between subsidies and grants in most cases, instead discussing all government transfer payments under a single category. DHS' research does make the distinction, however, and finds it meaningful.

3.4.10. Tax Incentives

Respondents also noted the use of tax incentives in encouraging behavioral changes, such as the residential energy tax credit and the first-time home buyer credit, and the potential effectiveness of such incentives in reducing the fixed costs associated with cybersecurity investment. Among suggested tax incentives were the accelerated depreciation of cybersecurity-related hardware and software, as well as tax credits and deductions for cyber-related personnel, and capital investment for organizations choosing to adopt the Cybersecurity Framework. A respondent from the financial sector suggested tax incentives based upon Statement of Position 98 of the Financial Accounting Standards Board, which provides guidance in accounting for the costs of computer software. Under this model, costs associated with Framework adoption could be tax deductible or amortized over a specific period of time. Uniquely, a respondent also suggested that tax incentives be provided to non-critical infrastructure businesses that contract with Framework adopters, providing a market incentive to further encourage Framework adoption among critical infrastructure owners and operators. Another respondent suggested a "Capital Gains Tax Incentive for Cyber Assurance that would reward shareholders with a lower capital gains tax rate on the sale of assets (stocks and bonds) of corporations that voluntarily adopt the NIST Cybersecurity Framework."

Table 3. Commerce Notice of Inquiry Responses by Incentive Category

Key

- ● Indicates the incentive was recommended by the respondent
- ○ Indicates the incentive was discussed but not recommended by the respondent
- ☐ Indicates the incentive was neither discussed nor recommended by the respondent

Commerce NOI Respondent		Grants to Unregulated Industries	Rate-Recovery for Price Regulated Industries	Insurance	Liability Considerations and Legal Benefits	New Legislation: Cyber SAFETY Act	Prioritized Technical Assistance	Procurement Consideration	Public Recognition	Security Disclosure	Streamline Information Security Regulations	Subsidies	Tax Incentive
1	Advanced Cybersecurity Center	●		●									
2	American Association for Laboratory Accreditation								○				
3	American Fuel and Petrochemical Manufacturers	○	○	●	●	○						○	○
4	American Gas Association	●	●		●								
5	American Insurance Association			○					●		○		
6	American Petroleum Institute				○		○				○		
7	American Public Power Association				●						○		
8	atsec							○			○		○
9	Booz Allen Hamilton	○		●	○				●		○		
10	Bryan Rich												
11	Business Software Alliance			●									●
12	CACI				○			●			●		

	Commerce NOI Respondent	Grants to Unregulated Industries	Rate-Recovery for Price Regulated Industries	Insurance	Liability Considerations and Legal Benefits	New Legislation: Cyber SAFETY Act	Prioritized Technical Assistance	Procurement Consideration	Public Recognition	Security Disclosure	Streamline Information Security Regulations	Subsidies	Tax Incentive
13	Covington & Burling/Chertoff Group				●	●		●			○		○
14	DCS Corp			●									
15	Donald Edwards								●				
16	Dong Liu			○	●				●			●	
17	E8dison Electric Institute				●								○
18	Electric Power Supply Association		●										
19	Emmanuel Adeniran	○			●		●					○	
20	Encryptics			●								●	
21	FCC				○						○		●
22	Financial Services Sector Coordinating Council	●			●						●		●
23	Gary Fresen				●								
24	Honeywell				●		●						●
25	Internet Infrastructure Coalition				●						●		
26	Internet Security Alliance	○	○	○	●	○	○	○	○	○	○	○	○
27	IT SCC				○							○	
28	Los Angeles Department of Water and Power	●		●	●		●					●	
29	Marsh			●									
30	Microsoft			●				●			●		
31	Monsanto				○								

	Commerce NOI Respondent	Grants to Unregulated Industries	Rate-Recovery for Price Regulated Industries	Insurance	Liability Considerations and Legal Benefits	New Legislation: Cyber SAFETY Act	Prioritized Technical Assistance	Procurement Consideration	Public Recognition	Security Disclosure	Streamline Information Security Regulations	Subsidies	Tax Incentive
32	National Cable and Telecommunications Assoc.				●			●			●		○
33	National Electrical Manufacturers Association				●			●					
34	National Rural Electric Cooperative Association			●	●	●							
35	NCTA- The Rural Broadband Association				●								
36	Robin Ore	●		○	○								○
37	San Diego Gas & Electric and Southern California Gas Company		●		●			●		●			
38	Sasha Romanosky			●	○					○		○	●
39	Southern California Edison										●		
40	Telecommunications Industry Association			●	●								●
41	Terrence August & Tunay Tunca				●				○			●	
42	U.S. Chamber of Commerce				●	●		●			●		
43	US Telecom Association	●	○		●	○	○			○	●	●	
44	Utilities Telecom Council				●						●		●
45	Voxem Inc.												●