Executive Order 13636: Improving Critical Infrastructure Cybersecurity

Department of Homeland Security Integrated Task Force

Incentives Study

June 12, 2013

Homeland Security

Background

The government and the private sector have a 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 measureable 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.

The Department of Homeland Security (DHS) recognizes the importance of market-based incentives in promoting change in business practices and encouraging the development of markets such as cyber insurance to promote adoption of the Cybersecurity Framework (hereafter, "Framework") required under Executive Order (EO) 13636. The Federal Government is also able to offer incentives in order to influence markets and facilitate the adoption of increased security practices, and this report summarizes their potential applicability to Framework adoption. In order to ensure that this report reflects the expertise of the entire homeland security enterprise, DHS actively sought advice from its partners in the private sector and across the government in addition to conducting an in-depth literature review.

Analysis

The DHS study methodology included the following phases: review of known cybersecurity incentive proposals; a literature review of evaluations of voluntary non-cybersecurity programs; stakeholder interviews and workshops; a review of responses to the Department of Commerce Notice of Inquiry.[1]

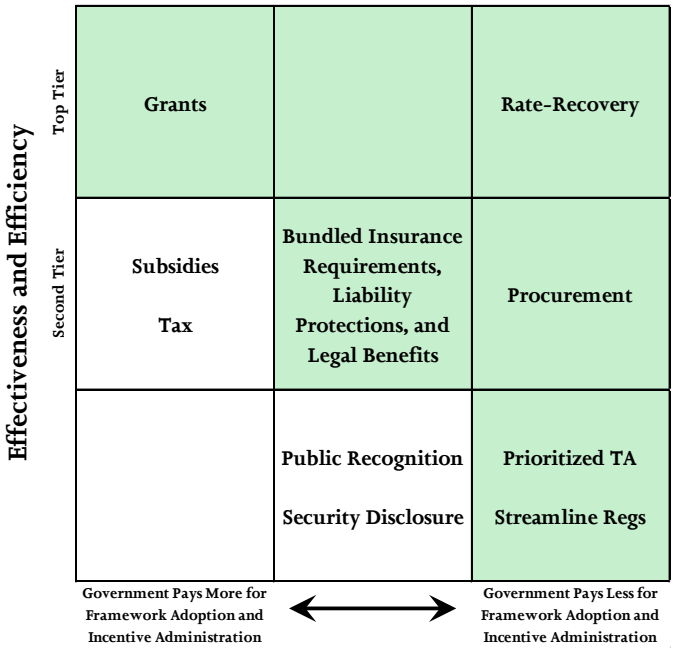
For the purpose of this study, DHS used the following definition of incentive: ***a cost or benefit that motivates a decision or action by critical infrastructure asset owners and operators to adopt the Framework under development by National Institute of Standards and Technology (NIST).*** The study considered a wide range of possible incentives that the Federal Government could use—either under existing law and authorities or only with new legislation—to encourage the investment required for adoption of the voluntary Framework.

It is important to note that while the incentives study was required within 120 days of the date of EO 13636, the preliminary version of the Framework is required within 240 days of the date of EO 13636. In addition, DHS will be establishing a voluntary program to support Framework adoption within 365 days of the signing of EO 13636. This report is limited by the current understanding of what the Framework will entail and would benefit from more specifics to inform the analysis and recommendation of the incentives designed for promoting its adoption. For example, knowledge of the Framework would allow the cost of Framework adoption to be quantified. Since the Framework is still under development, this was not possible, and so the incentives considered were evaluated at a more general level with the understanding that the analysis would be updated as needed as the Framework is developed. Since the Framework is still in development at the time of this writing, the incentives that are intended to promote its adoption were assessed prospectively, in terms of the likelihood that they will motivate organizations to adopt the Framework in the future. It is expected that the most effective incentives will not only promote adoption of the Framework, but they also will motivate adopters to implement higher levels of cybersecurity

[1] A detailed description of the methodology and analysis used for this report can be found in the DHS Incentives Study Analytic Report at http://www.dhs.gov/publication/analytic-report-executive-order-13636-cybersecurity-incentives-study.

standards, methodologies, procedures, and processes within the Framework, and ultimately generate greater confidence in the overall level of the nation's cybersecurity.

DHS evaluated potential incentives in terms of three economic criteria – effectiveness, efficiency, and equity – while remaining cognizant of feasibility in terms of costs and policy considerations. In general terms, each of these criteria answer the following questions: (1) Effectiveness—does it work? (2) Efficiency—is there waste? (3) Equity—who pays and how much? Using the broad range of information sources gathered in our research, each incentive was qualitatively assessed in relative terms against each of these criteria using the following simple tiering heuristic: (1) top tier incentive, relative to other incentives, against each criterion; (2) second tier incentive, relative to other incentives, against each criterion; or (3) insufficient evidence to merit either a top tier or a second tier assessment, relative to other incentives, against each criterion. The figure below summarizes the results of the analysis of each of the incentives considered against the criteria above. Because the tiering assessments for effectiveness and efficiency were identical, these criteria were consolidated in a single tiering assessment on the vertical axis.



Recommendations

DHS recommends that the Administration continue analysis of the menu of six incentive categories below. While DHS is not able to offer specific recommendations on implementing these incentives categories at this time, the Department has conducted an initial analysis regarding legal feasibility and recommends that such analysis continue and lead to specific policy and implementation proposals. The following menu of six incentives categories are recommended for further analysis:

- **Grants**: fixed cost, performance-based awards for investment in cybersecurity products and services for prospective Framework adopters. In addition to consideration of a new grant program, consideration could be given to directing the utilization of existing Federal grant programs through existing or new statutory authority. As an alternative to awarding grants as described, agencies could require critical infrastructure projects funded through Federal grants to adopt the framework. Current grant authorities and appropriations might provide some flexibility for DHS or other Federal agencies, but it seems more likely that new statutory authority would be required to

implement this particular type of incentive in a comprehensive and large scale way. DHS should be one of several agencies implementing this incentive.

- **Rate-Recovery for Price-Regulated Industries**: recovery of cybersecurity investments in the rates charged for services provided by Framework adopters through a price cap, in which the government allows a firm to charge up to a certain maximum price that is independent of the realized cost. An initial incentive could be applied to prices of transportation services provided by interstate natural gas pipeline companies using Federal Energy Regulatory Commission (FERC) authorities. Existing legal authority, with additional FERC action, may be sufficient. Note, however, that most price-regulated industries are regulated by States and municipalities and the nature of Federal incentives for these entities requires further consideration.
- **Bundled Insurance Requirements, Liability Protection, and Legal Benefits**: a system of litigation risk mitigation for which those entities that adopt the Framework and meet reasonable insurance requirements are eligible to apply. Other types of legal benefits may include limited indemnity, higher burdens of proof, or limited penalties; case consolidations; case transfers to a single Federal court; creation of a Federal legal privilege that preempts State disclosure and/or discovery requirements for certain cybersecurity self-assessments. Insurance options could include a requirement for the purchase of private market liability insurance in order to apply for these liability protections and legal benefits. New statutory authority would likely be required.
- **Prioritizing Certain Classes of Training and Technical Assistance**: the Federal Government offers several types of technical assistance to critical infrastructure owners and operators, including preparedness support, assessments, training of employees, and advice on best practices. The primary criteria for assistance should remain criticality and security and resilience gaps, and owners and operators in need of incident response support will never be denied assistance based on whether they have adopted the Framework. However, for some non-incident response programs Framework adoption should be explored as a secondary criterion for prioritizing the order in which assistance is provided. Existing authority is considered sufficient, as determining the allocation of government resources among similarly situated critical infrastructure entities is primarily a question of policy and resource prioritization.
- **Procurement Considerations**: introduce a technical requirement in the procurement process for certain types of acquisitions for Framework adopters, or requirements for Framework adoption for Federal information and communications technology providers or other contracts, particularly those involving access to sensitive government information or essential services. This may include leveraging existing authorities, using incentives, and modifying the Federal Acquisition Regulation.
- **Streamline Information Security Regulations**: consider the creation of a unified compliance model for similar requirements and eliminate overlaps among existing laws; streamlining of differences between U.S. and international law (perhaps through treaties); ensuring equivalent adoption; reducing audit burdens; and offering prioritized permitting.

In addition to recommending further study on each of the incentives categories above, DHS also supports the call from the National Science and Technology Council's Subcommittee on Networking and Information Technology Research and Development (NITRD) for additional research to "Explore models of cybersecurity investment and markets; Develop data models, ontologies, and automatic means of anonymizing or sanitizing data; Define meaningful cybersecurity metrics and actuarial tables; Improve the economic viability of assured software development methods; provide methods to support personal data ownership; and Provide knowledge in support of laws, regulations and international agreements."