DHS Incentives Study: Preliminary Analysis and Findings

Executive Order 13636 on Improving Critical Infrastructure Cybersecurity

Tony Cheesebrough
Chief Economist
National Protection and Programs Directorate and
Integrated Task Force for EO 13636 and PPD-21

June 21, 2013

Homeland Security

Cybersecurity Incentives Study Requirements

- The Executive Order (EO) requires the Secretary, within 120 days (by June 13), to make recommendations to the President on:
  - "a set of incentives designed to promote participation in the [cybersecurity] Program…", including an "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."
- Though the EO requires separate studies from DHS, Treasury, and Commerce, the DHS Integrated Task Force (ITF) has been working collaboratively with these partners to share data, research, and analysis to produce its study
  - The White House Council of Economic Advisors, Treasury Tax Policy and Insurance Policy Offices, and Homeland Security Institute each provided focused secondary research support
  - For its report, Commerce is reviewing the feasibility of recommendations made in response to its Notice of Inquiry (NOI)

Homeland Security

Final List of Incentives Considered

	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

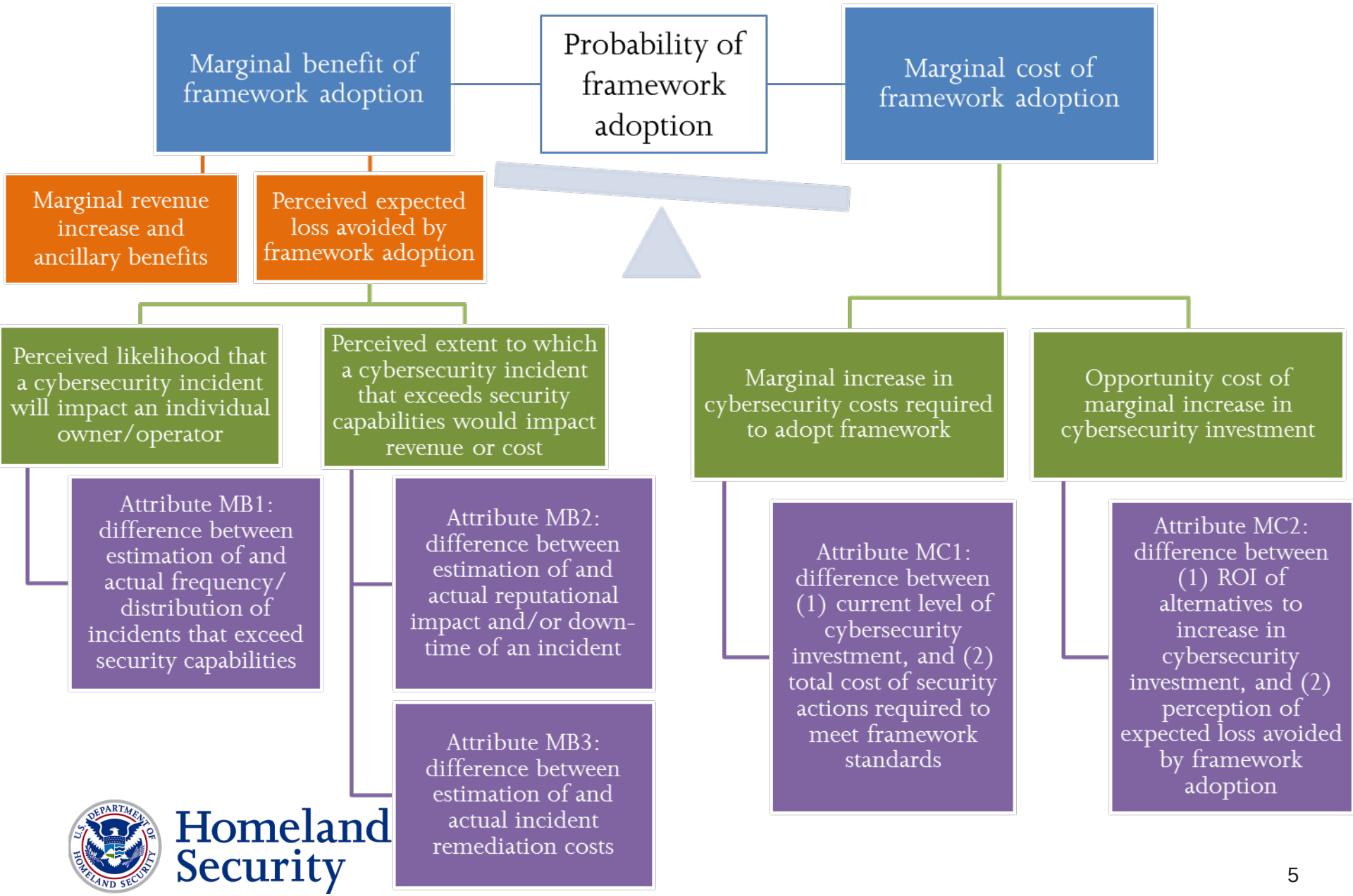
Homeland Security

Research Methodology

- Definition. For the purpose of this study, DHS will use the following definition of incentive: a cost or benefit that motivates a decision or action by critical infrastructure asset owners/operators to adopt the cybersecurity framework under development by NIST.
- Central Researchable Question. To what extent would each of the incentives under consideration affect the probability that critical infrastructure asset owners/operators will adopt the cybersecurity framework under development by NIST?
- Basic Methodology. Without better data, a basis for quantitative estimates of the benefits of cybersecurity incentives is lacking, and until the EO-required framework is developed by NIST, the same is largely true of the costs of implementing the framework.
  - As a result, the methodology for analyzing the effectiveness of the cybersecurity incentives under evaluation for the EO relied on evaluations of voluntary non-cybersecurity programs and largely qualitative methods.
  - Evaluations of incentives applied to voluntary non-cybersecurity programs are assumed to be relevant to the study of voluntary cybersecurity programs, though identical results were not assumed.
- Information Sources.
  - Literature review completed with research support from the Council of Economic Advisers, Treasury Tax Policy and Insurance Policy Offices, and Homeland Security Institute, yielding 138 peer-reviewed journal articles, law review articles, conference papers, working papers, government reports, dissertations, and book chapters.
  - DHS/ITF Incentives Workshop: completed April 19, 2013
  - U.S. Department of Commerce Notice of Inquiry (NOI): completed review of 43 comments

Homeland Security

Microeconomic Framework



Homeland Security

Economic Criteria for Analysis

- Effectiveness: does it work?
  - Effectiveness is the probability of framework adoption and is principally driven by framework cost sharing, though expected loss avoidance, marginal revenue increase, and ancillary benefits also contribute to a lesser extent.
- Efficiency: is there waste?
  - Efficiency applies to cost sharing incentives, and consists of both:
    - Moral hazard, which 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/operators to choose techniques that are not cost-effective; and
    - Adverse selection, which in this context exists due to differences in the cost of adoption among owners/operators within and across sectors, and can be thought of as over-paying "lost cost" owners/operators which are already near the frontier of sophistication.
- Equity: who pays and how much?
  - Government, industry, or consumers; all/most, moderate, or none/least.

Homeland Security

Preliminary Analysis

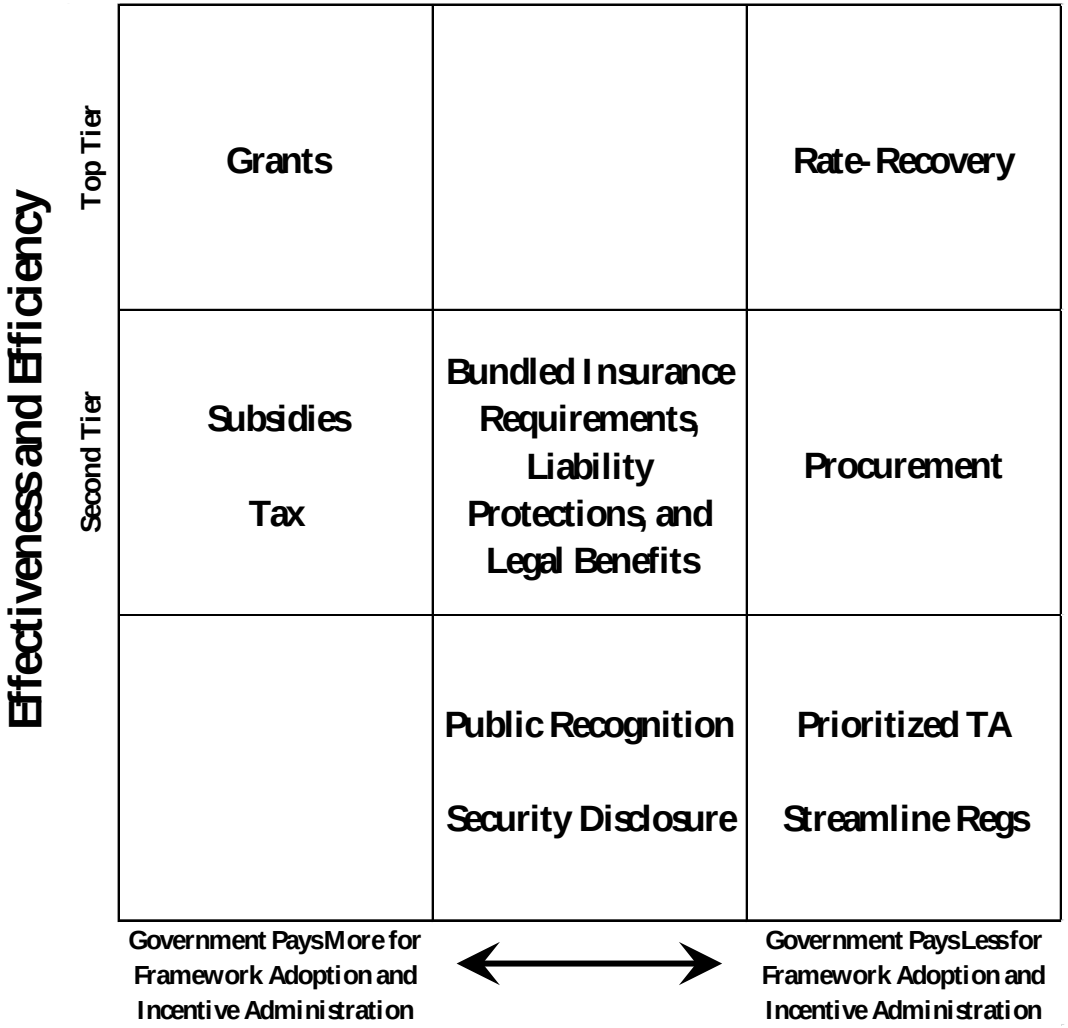
	Incentive	Effectiveness				Efficiency		Equity		
		Probability of Framework Adoption	Framework Cost Sharing	Expected Loss Avoided	Marginal Revenue Increase and Ancillary Benefits	Moral Hazard	Adverse Selection	Government/ Taxpayer Cost	Industry Cost	Consumer Cost
1	Grants	●	●			●	●		●	●
2	Rate-Recovery 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 either 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.

Homeland Security

Preliminary Findings



- Grants: most effective and efficient with least industry cost but highest government cost
- Rate-Recovery for Price-Regulated Industries: most effective and efficient with least government and industry cost but highest consumer cost
- Bundled Insurance Requirements, Liability Protections, and Legal Benefits): moderate effectiveness with moderate government cost
- Prioritized Technical Assistance: moderate expected loss avoidance with least government cost
- Procurement Considerations: moderate effectiveness for least government cost
- Public Recognition: little evidence of effectiveness independent of procurement requirements and potential for unintended consequences such as cyber targeting
- Security Disclosure: little evidence of effectiveness and potential for unintended consequences and perverse incentives
- Streamline Information Security Regulations: ancillary benefits with least government cost
- Subsidies: less effective than other cost-sharing incentives and inefficient due to moral hazard with highest government cost
- Tax Incentives: less effective than other cost-sharing incentives and inefficient due to moral hazard with highest government cost

Homeland Security

Proposed Procedure for Awarding Incentives

- In practice, it might difficult for DHS to determine whether the framework has been adopted, particularly when incentive awards are based on that determination.
- A more practical solution might be for DHS to follow procedures whereby applicants are evaluated on the extent to which they have adopted a standard.
  - This is also consistent with the administration's "*Pay for Success"* model of payment for performance in the context of social services.
- In this way, either the size of the incentive would be made contingent on the evaluation, or a penalty would be assessed for a low evaluation.
- Owners/operators would be awarded with higher levels of incentives for improving their evaluations, and since it is not tied to cost, moral hazard is eliminated.
- Adverse selection is also addressed, because even a "high cost" owner/operator with a low level of cybersecurity sophistication can be motivated to improve.
  - "Low cost" owners/operators, already near the frontier of sophistication, stop receiving incentives once they reach the highest level of evaluation, though penalties may be assessed for regression.

Homeland Security