Abstract
A look at the United States Government proposed incentives for adoption of the Cybersecurity Framework and higher cybersecurity standards while focusing on their potential impact on business and information sharing.
Introduction

On February 12, 2013 the President signed an Executive Order titled *Improving Critical Infrastructure Cybersecurity*\(^1\) that contained guidance and requirements for a number of efforts that would help the owners of critical infrastructure secure their operations against cyber-attacks. The Executive Order called out the creation of a “Baseline Framework to Reduce Cyber Risk to Critical Infrastructure” which would be an industry driven document led on the Government side by the National Institute of Standards and Technology (NIST). To help drive the adoption of the Framework once created, a Voluntary Program will be established that would be run by the Department of Homeland Security and would find ways to promote the Framework and incentivize participation. Specifically in Section 8d of the Order, a set of incentives to promote the Program are to be created by the Department of Treasury, Department of Commerce, and Department of Homeland Security. As described in the Order, these incentives had to be done in 120 days while the draft Framework had to be published in 240 days so the proposed incentives had to be given without detailed knowledge of the draft Framework. Now that the draft version of the Framework is available, it is a good opportunity to review the proposed incentives to try and determine which are well aligned with industry information sharing, the current security environment, and the draft Framework.

With the focus on the Framework, information sharing, and effectiveness, proposed incentives from all three agencies were reviewed to see which incentives could be valuable if implemented and which ones were less likely to promote adoption and improvement of cybersecurity. While all potential incentives were reviewed, detailed analysis will only be provided for some due to similarity. Each agency proposed separate incentives based on their areas of expertise and perceived needs and as shown by the table below, there were significant overlaps and even disagreements. The overlaps and disagreements are a positive sign as the agencies look at the same challenges and see more than one potential way to deal with them. While the incentives are not very detailed at this point, an incentive area that is mentioned by all three agencies seems more likely to be included in the final incentives when they are developed. A number of incentives were agreed upon by two or even all of the agencies but only two incentive areas resulted in disagreement and one of those disagreements is more related to agencies talking about the role of Government.

---

**Summary of Proposed Incentives**

<table>
<thead>
<tr>
<th>Incentive Area</th>
<th>Treasury</th>
<th>Commerce</th>
<th>DHS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clarify Liability Risk</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cybersecurity Research / Grants</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Technical Assistance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Include in Procurement Language</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Streamline Regulations</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Cyber Insurance</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Information Sharing</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rate Recovery for Regulated Industries</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Fast Track Patents for Cybersecurity</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Public Recognition Program</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Accelerated Security Clearance</td>
<td>✓</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Tax Breaks</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

The incentive areas related to liability risk, research and grants, and technical assistance were mentioned by all three agencies. These are particularly interesting because some of them were not mentioned often in RFI responses and the three are seemingly unrelated. At the start of this effort, it was possible that perhaps incentives with the most mention would be financial options such as tax breaks, grants, procurement language, or rate recovery. Or maybe incentives focused more on operational effectiveness would be mentioned by focusing on information sharing, technical assistance or streamlining regulations. Finally another trend could have been the emphasis of legal or policy incentives with insurance, liability, and risk incentives being the most popular. But each agency chose incentives that were not easily grouped and did not follow a trend or pattern.

Organizations are reviewing the Framework and other published information and providing RFI responses to NIST as a result of the Executive Order. These responses indicate that industry is looking for improved information sharing. One of the major challenges mentioned in the RFI responses as well from our interviews with firms is the issue of liability. If an organization shares information with another company or the Government it is crucial to know who is responsible for that information, how it is used, and how it is protected. If an organization may be considered liable for information it shares it is much less likely to trade information. Whether the agencies submitted clarifying risk as an incentive because they want organizations to share information with the government, or because they see the need for sharing between companies and know that liability is a major challenge, it is a positive sign that all three agencies proposed incentives to address liability.

The second overlap of proposed incentives is the adoption of the Framework and participation in the voluntary program as an advantage in the grant award process and in research opportunities.
Based on our research of the RFI responses and interviews with organizations, grants and research funding and technology were not mentioned as limiting factors. However, an open question is whether the departments are promoting this incentive to target smaller or less mature organizations. Awarding bonus bidding points to organizations that adopt the Framework may not result in higher cybersecurity standards. That will unquestionably reward organizations that claim they have adopted the Framework. Since all agencies mentioned it in their proposals, one can expect the final incentive suite will include criteria that more directly supports improved cybersecurity versus self-attestation of adopting the framework.

The final common incentive area across the three agencies was more opportunities for technical assistance. Currently technical assistance is offered to some critical infrastructure owners so this would be an extension of the existing efforts. Technical assistance was not mentioned in many RFI responses but this assistance may be crucial for adoption by smaller or less mature organizations. As the Framework and all information related to the Executive Order was supposed to be applicable for organizations of all sizes, this incentive area may be more focused towards the small and medium sized business.

In addition to the three common incentive areas between the three agencies, there were also two proposed incentives that agencies disagreed with each other on. The first incentive was for accelerated security clearances. The Department of Treasury thought this was a valuable incentive while the Department of Commerce thought it should not be considered. It could be that the financial sector does not have enough cleared people to process classified threat information and to participate in information sharing, but I believe that the Department of Commerce was correct in their judgment to not consider it further. Additional information on each of the agencies and their potential reasoning can be found in the individual agency sections below but with the recent insider physical attack at the Navy Yard\(^2\) and the well-publicized information leak by Edward Snowden\(^3\) the image of expediting security clearances may not be well received by the public. On the positive side, this may be another incentive area that is more focused on smaller businesses. Large businesses and organization that regularly interact with the Government may have security offices and are familiar with the forms and procedures, while a smaller firm would not have these advantages. So by expediting the clearances, it would help smaller firms gain access to the same information the larger firms have, but could introduce additional


security concerns if these firms do not have the procedures and practices in place to protect this information.

The other disagreement came from the proposed incentive around cyber insurance. Cyber insurance is a popular topic in cybersecurity discussions today as it is a hard subject but an important one. The disagreement between the agencies does not come from arguing over the importance of cyber insurance, but the role of the Government in it. The Department of Treasury recommended that cyber insurance not be included as an incentive because they do not believe Government needs to play a role in the industry. The Department of Commerce and Homeland Security both propose an incentive that seemingly aligns the insurance industry and the Framework and the adoption program. When incentives come out as part of the voluntary program, we believe that cyber insurance will be included and the Government will have to determine the right role for it in the cyber insurance environment.

After looking at the incentives at the Government level, it is valuable to look at the individual agencies and what they proposed to get an idea of their current thoughts on cybersecurity and where they see the effort going in the future.

**Department of Treasury**

The Department of Treasury report outlines the perspective of the Department in terms of what criteria they believe are important for an incentive to be successful. After putting seven potential incentives through their criteria, they determined that five were acceptable and two were not. An interesting part of their approach is that they believe that many of the recommendations in the Framework and in the incentives would not just apply for critical infrastructure owners, but also for many private organizations that are looking to improve their cybersecurity. The other two agencies only mention critical infrastructure organizations in their reports which is one difference between the agencies. Before reviewing the five potential options and two rejected options, it is important to understand the criteria that the Treasury Department used when they reviewed potential incentives. The criteria that the Treasury Department used to review the seven potential options were to ensure the incentives:

1. Be Appropriately tailored and scaled to the magnitude of under-investment in cybersecurity
2. Protect taxpayers by being cost effective while still achieving the policy objectives
3. Adjust to changing circumstances and the availability of new information
4. Be coordinated, so as not to duplicate other incentives
5. Motivate private sector entities to expend their own resources to further protect their critical infrastructure assets.\(^4\)

While all of the criteria were important, the inclusion of language around the incentives being tailored and scaled as well as adjustable is especially important with an effort like this that applies to so many different organizations. Huge urban power generation companies may have the resources to implement advanced security or at least have pieces in place. Smaller cooperatives may not have as advanced security in place but they also may not have the same risk exposure. NIST designed the Framework for flexibility and thus the incentives also need to be flexible around the different risks of critical infrastructure organizations.

The seven potential incentives that the Department of Treasury proposed can be found in the Appendix. Out of the five recommendations that Treasury kept as potential options, one of them stood out as particularly important as it specifically called for information sharing. This emphasis on information sharing was also mentioned in many of the RFI responses to NIST at the start of the Framework drafting process and in House and Senate Committee meetings that discussed new cybersecurity legislation. The response to Senator Rockefeller of the Senate Commerce Committee from the Financial Services Sector Coordinating Council (FSSCC) stated that information sharing was the most critical line of defense in mitigating cybersecurity risk in their industry.\(^5\) The proposed incentive states that if the Framework and associated efforts can improve information sharing then the Framework would be much more valuable to industry and industry would be more likely to adopt it. One way Treasury believes that the Framework can achieve this is by helping to standardize practices and improve current guidelines. This stood out because it echoes some of the thinking from the NIST writing team for the Framework. The hope is that by providing a core with categories and sub categories and references in the Framework, the language used around cybersecurity, at least within critical infrastructure, will start to standardize. If language becomes more common it will be easier for organizations to communicate with the Government and with each other which will make adoption of the Framework much more appealing. This improved information sharing also will work outside of critical infrastructure as anyone who wants to adopt the commonly used terms and definitions will be


better able to communicate with any other user of the Framework and hopefully the standard terms and definitions would eventually become common usage and understanding.

In addition to the five incentives that Treasury proposed, they also rejected two inventive areas that had been under consideration. The recommendations that were removed was an incentive around tax breaks and one on cyber insurance. The removal of the tax breaks incentive was echoed by another agency and both agencies mentioned the challenges of implementing these tax breaks due to the complexity of cybersecurity. A tax break would be very hard to tie purely to cybersecurity as tying it to adoption would lead to potentially more adoption without improved security. Moreover, how would an improvement in security be measured to justify a tax break? Until better metrics for cybersecurity are agreed upon and adopted tax breaks will not be a good incentive. The removal of the second incentive, cyber insurance, seems to place the Department of Treasury against the other agencies but the agencies in disagreement over the appropriate role of Government, not the value of cyber insurance as an incentive. The Department of Treasury believes that Government does not need to interfere with the development of a private market for cyber insurance. At this point there is not a large market for cyber insurance, but with the increasing emphasis on cybersecurity and the potential threats, private industry is already beginning to fill this need. The other agencies have incentives around cyber insurance that are more related to the liability and clarification of risk. If the Framework and other EO efforts can help determine risk and clarify liability for information sharing then that would help the cyber insurance market however it develops. Cyber insurance providers will develop liability and risk models as they have in many other industries, but any clarification from EO efforts would be a valuable step and would improve the quality and accuracy of insurance organizations can buy.

Because the Framework draft was just posted and the comment period just opened, the incentives are one way to see how the agencies think about cybersecurity. As the Treasury did not mention streamlining regulations, a public recognition program, or rate recovery it appears that Treasury views the role of the agencies as supporting and allowing business to determine the direction. By clarifying liability and promoting information sharing Treasury believes the Framework and related guidance should support what businesses are already doing and not attempt to change this. This idea of supporting the private sector does not appear to be in complete alignment with DHS which will be discussed later as DHS seems to want more direct involvement and it will be interesting to see which incentives get offered.
Department of Commerce

The Department of Commerce was in an interesting position to propose incentives as NIST is leading the effort to write the Framework and is also part of the Department of Commerce. After reviewing the incentives that were proposed it does not appear that the two efforts were overlapping as the criteria was not Framework focused and was very broad. The criteria used are listed below:\(^6\):

1. Promote participation in the Framework
2. Involve judicious commitment of any additional federal government resources
3. Advance a full range of policy interests, including protecting privacy and civil liberties
4. Promote effective cybersecurity for critical infrastructure entities

At the end of their review, Commerce proposed ten potential incentive areas and rejected two from consideration and the full list can be found in the Appendix. The list of ten incentives are more theoretical than the proposals from Treasury with recommendations like “study tort liability” and “ensure that research and development is linked to real cybersecurity problems.” For comparison, Treasury said “clarify liability” and “provide grants for cybersecurity research.” The Department of Commerce’s flexible recommendations come from the interaction between Department of Commerce and their stakeholders throughout the development of the incentives and possibly a core belief that standards should be led by the private sector. While almost everyone agrees that it will require a public-private partnership, Commerce reached out to stakeholders to get feedback on potential incentives before they even proposed them as a draft. Willingness by Commerce to support the private sector is a good idea and if the private sector agrees on the incentives then it should encourage adoption of the Framework.

The specific proposed incentive areas are generally similar to the incentives proposed by DHS and Treasury as seen in the summary section above. Commerce also agreed with Treasury that tax breaks were not a reasonable incentive and should not be considered. Commerce did not exactly agree with Treasury on the incentive area of cyber insurance but as was discussed in the Treasury section, the Department of Commerce is more focused on the development of the Framework while Treasury was more focused on the functioning of the market after the Framework is in place. This is another example of the perspective of the two agencies as Commerce is more theoretical and wants to slowly develop the specific direction and guidance while Treasury wants to focus on a few key areas, information sharing and liability, and tie the Framework to those areas. Another example of Commerce emphasizing

the public-private partnership is the proposed incentive that participants in the voluntary program get
an advantage in the awarding of grants and especially NSTIC pilot projects. The National Strategy for
Trusted Identities in Cyberspace (NSTIC) is a Department of Commerce led effort that involves the
improved interoperability and use of credentials for the general public and up to this point has not been
directly tied with the Department of Commerce effort around critical infrastructure. This incentive is
unlike the other Department of Commerce proposals. It is very specific. If Commerce can find an
incentive that supports the adoption and awareness or two of its largest projects related to
cybersecurity that is a positive step. Overall, the Department of Commerce proposed incentives seem to
be a collection of inputs from stakeholders with limited Commerce specific information, but the
incentives are a clear example of the mindset of Commerce around this effort that this must be a public-
private partnership to be successful.

**Department of Homeland Security**

The Department of Homeland Security proposed recommendations based on criteria that were
focused on the economics of potential incentives. They evaluated incentives based on:

1. Effectiveness – does it work?
2. Efficiency – is there waste?
3. Equity – who pays?

In addition to these criteria, DHS also considered the feasibility of implementation as well as policy
considerations and developed a matrix of effectiveness and cost to give them a tier system. This tier
system included the six recommended policy areas, including an incentive called bundled insurance
requirements, liability, and legal benefits which represents multiple check marks in the summary table,
as well as other potential incentives that did not meet their criteria. The method that DHS used is clear
and provides a way to rank potential incentives based on different criteria. Some of the measurements
they claim are open to interpretation. Better metrics would improve the matrix. For example, Grants
are in the more expensive category, but Grants are already being given out and some of the existing
grant money could go towards cybersecurity making it cost neutral. Perhaps they are talking about
overall cost, not about additional or new costs. Below is the matrix that DHS filled out and additional
information is below the diagram.

---

7 Department of Homeland Security, Cybersecurity incentives study,
http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-summary-report-cybersecurity-incentives-
study_0.pdf
As shown above\(^8\) in the matrix, grants and rate recovery were the top most effective incentives. This ranking gives us a good idea of the mindset of DHS around cybersecurity and the Executive Order efforts. DHS was the only agency to propose rate-recovery which seems a little more prescriptive and mandatory than a lot of the other proposals. DHS has a lot of experience in cybersecurity which may be the reason they are comfortable being more direct. Their top tier also shows how DHS feels about the public private collaboration which seems to be different than Commerce. While Commerce was very open and seemed prepared to let the private sector lead, DHS seems like they want Government to take the lead and direct the private sector through grants and rate recovery for organizations using the Framework and approved methods. Also shown in the matrix are recommendations that DHS is not considering but other agencies did such as the public recognition program that Commerce recommends, and tax breaks which all three agencies are not considering moving forward. Overall, the DHS method of looking at the incentives provides a useful framework for rating the likelihood of success of a given set of incentives.

The proposed incentives from Department of Treasury, Department of Commerce, and Department of Homeland Security, while being somewhat vague and only in draft status offer an

---

opportunity to see the direction and perspective of these agencies on cybersecurity. These incentives are especially important because they seem to show how the different agencies feel about the role of Government and the role of the private sector. Department of Commerce seems to want to take a supporting role and let the private sector drive the process and results while the Department of Homeland Security wants to lead the effort and help guide the private sector in the direction they believe is best. It will be extremely interesting to see how the incentives are finalized as part of the Voluntary Program and to see how they will change when the Framework and comments to the Framework from the private sector become available.
Appendix: Full lists of the Incentives
Department of Treasury

1. Enhancing Information Usage Capabilities to Support Information Sharing
2. Leveraging Framework Adoption to Clarify Liability Risk
3. Government Funding for Basic Cybersecurity Research
4. Providing Technical Assistance
5. Further Accelerating the Security Clearance Process
6. Tax Incentives (removed from consideration)
7. Cyber Insurance (removed from considerations)
Department of Commerce

1. Engage insurance companies in the creation of the Framework
2. Study tort liability
3. Consider participation in the program as a criterion for NSTIC pilots and other commerce grants
4. Offer guidance to federal agencies on compliance with the Framework and participation in the federal grants program
5. Ensure that the Program links research and development to overcoming real-world challenges
6. Identify Candidates for regulatory streamlining
7. Explore a fast track patent pilot for cybersecurity
8. Study the use of government procurement considerations
9. No further study on the use of tax incentives (removed from consideration)
10. Study the development of an optional public recognition program for participants in the Program
11. Explore providing specific types of technical assistance to participants in the Program
12. Further steps should not be taken to provide expedited clearance to Program participants (removed from consideration)
Department of Homeland Security

1. Grants
2. Rate-recovery for price-regulated industries
3. Bundled insurance requirements, liability protection, and legal benefits
4. Prioritizing certain classes of training and technical assistance
5. Procurement considerations
6. Streamline information security regulations