Treasury Department
Summary Report to the President on

Cybersecurity Incentives
Pursuant to Executive Order 13636

SUMMARY REPORT AND RECOMMENDATIONS

The cyber threat to our nation's critical infrastructure is growing and represents one of the most significant challenges facing the United States. On February 12, 2013, President Obama signed Executive Order 13636, directing the federal government, in conjunction with the private sector, to develop a "Cybersecurity Framework"(hereinafter, "the Framework"). The Executive Order also directed the Secretary of the Treasury to identify and recommend a set of incentives that would encourage critical infrastructure organizations to adopt the Framework.

This report is the result of that effort, and its findings may be applicable not only to critical infrastructure organizations but also to a broader group of private sector participants. The report lays out an approach for policymakers to evaluate government incentives in promoting the adoption of the Framework, and then briefly assesses seven potential policy options in areas where the Treasury Department has significant or recent experience. It is not intended to provide an analysis of all available policy options.

The report outlines several principles for policymakers to use in assessing the benefits and relative effectiveness of government cybersecurity incentives. Generally, government incentives should be considered when private market incentives are insufficient to provide an appropriate level of cyber security. Ideally, these incentives should: (i) be appropriately tailored and scaled to the magnitude of the under-investment in cybersecurity; (ii) protect taxpayers by being cost-effective while still achieving the policy objectives; (iii) adjust to changing circumstances and the availability of new information; (iv) be coordinated, so as not to duplicate other incentives; and (v) motivate private sector entities to expend their own resources to further protect their critical infrastructure assets.

The report then applies these principles to the seven policy options identified below to assess their relative effectiveness as a government incentive. It describes the advantages and disadvantages of each policy option and attempts to evaluate the extent to which each would incentivize critical infrastructure organizations to improve cybersecurity. It also attempts to gauge the extent to which each policy option would encourage critical infrastructure organizations to voluntarily adopt the Framework, including whether additional legislation would be required. Engagement with critical infrastructure stakeholders, through formal comment letters and more informal panel discussions, helped to inform these findings.

Of the seven policy options that were evaluated, Treasury identified an initial set of five that warrant further consideration as government incentives following the issuance of the preliminary Framework. Although these policy options generally adhere to the principles above, full assessment of whether they could be effective incentives for encouraging adoption of the Framework must take place with reference to the terms of the Framework itself.

Recommendations Summary:

Enhancing Information Usage Capabilities to Support Information Sharing

Treasury recommends leveraging Framework adoption to encourage critical infrastructure organizations and other private firms to strengthen their cybersecurity practices in order to improve and increase the flow of real-time information between the government and private sector. This can be done by making sure the protocols and standards of the Framework promote information-sharing and that existing rules and guidelines pertaining to information-sharing are clear. Information that could be useful to improving cybersecurity, particularly in the context of an imminent or ongoing incident, should always be made available to affected firms. In other words, adoption of the Framework could lead to the creation of standard practices and policies, which would help critical infrastructure organizations and other private firms better utilize threat information for more timely and effective mitigation of cyber threats within their environments. Furthermore, many critical infrastructure stakeholders remain concerned about sharing information, citing concerns about potentially significant legal, reputational, competitive, or regulatory consequences. However, some of these concerns could be addressed through the clarification of existing rules and guidelines. Additional legislation may also be necessary.

Leveraging Framework Adoption to Clarify Liability Risk

Treasury recommends further study of whether adopting the Framework through the voluntary program could serve as a standard of conduct for, or minimum acceptable level of, systems integrity and precautions. Following particular practices contained in the Framework and joining the voluntary program could be used to clarify the assignment of liability, potentially by providing the basis for liability protections. A court may find that joining the voluntary program, implementing the Framework or, at the very least, some of its practices, satisfies a duty of care in a civil lawsuit. Alternatively, legislation could establish a statutory defense. Such a defense could take several forms. For example, it could take the form of a safe harbor, which could present a partial or complete defense from liability. Alternatively, it could take the form of a rebuttable presumption that a critical infrastructure entity has taken sufficient action under the circumstances. In either case, however, it is important to note that extending liability protection could also introduce moral hazard, undermining the policy objective of increasing cybersecurity to the extent critical infrastructure organizations are not held liable for taking insufficient precautions.

Government Funding To Encourage Basic Cybersecurity Research

Treasury recommends leveraging the Framework to promote existing federal grant programs that fund basic research pertaining to cybersecurity. This, in turn, could encourage innovation in cybersecurity and lead to products and practices that implement the Framework more effectively or efficiently for critical infrastructure organizations. Such innovations would promote framework adoption as well as generate a broad array of spillover benefits to other firms. To be sure, the potential benefits of basic research tend to have a longer time horizon and are uncertain. That means the effectiveness of using such research grants as an incentive to encourage adoption of the Framework may be limited.

In addition, the Framework could serve as an incentive if research proposals aligned with the Framework received preferential treatment for federal research funds. To increase the effectiveness of these research grants, agencies should use alignment with the Framework as a selection criterion. Research that is informed by, and intended to support, the Framework is more likely to lead to beneficial products and services. Given the potential interest, Treasury believes it would be beneficial to expand its current role as an "R&D liaison" between the financial services sector and government. No additional legislation would be required for Treasury to provide this service.

Providing Technical Assistance

Treasury recommends offering technical assistance to encourage critical infrastructure organizations to adopt the Framework and/or additional programmatic technical assistance to those who comply with the Framework's objectives. This would directly improve cybersecurity by providing additional government support beyond the context of incidents to critical infrastructure organizations seeking to configure their systems and address other threats.

Technical assistance would be well-targeted, immediate, and flexible enough to address changing cyber threats. Yet, doing so could introduce moral hazard if critical infrastructure organizations came to rely on the government before exhausting available private options for technical support. Policymakers must also reconcile such a program with the understanding that the federal government has a responsibility to provide technical assistance to any firm that requests emergency help. However, in non-emergency situations, the offer of *additional* programmatic technical assistance to encourage adoption and or implementation of the Framework would not conflict with this basic principle.

The use of technical assistance as an incentive could take several forms. During the implementation stage, any critical infrastructure organization seeking to adopt the Framework could be eligible for basic technical assistance regarding the implementation of measures that are consistent with Framework. This could lower adoption costs. Technical assistance could also be employed as an incentive after critical infrastructure organizations have adopted the Framework.

Under this scenario, critical infrastructure organizations that demonstrated they had adopted the Framework would have access to continued technical assistance and relevant information to facilitate compliance with the Framework. This could enable enhanced protection for cyber-systems. Additionally, when technical assistance is provided, source documents could point to the Framework and explain how its adoption could increase the security of the organization's systems. This could further serve as an incentive to encourage Framework adoption and compliance.

Treasury currently supports and facilitates technical assistance to the financial services sector by government agencies. Regardless of the form it takes, additional legislation would not be required for Treasury to continue or expand this role.

Further Accelerating the Security Clearance Approval Process

Treasury recommends exploring ways to further accelerate the security clearance approval process. Treasury recommends that the federal government put in place appropriate reporting requirements or other controls on federal agencies to assure the timely processing and approval of security clearance application requests for qualified individuals at all private sector firms, but particularly critical infrastructure organizations that are deemed eligible for prioritization under the Executive Order. Furthermore, Treasury recommends that the federal government be more active in educating critical infrastructure organizations and other private sector firms about the eligibility criteria and approval process for obtaining a security clearance. Taken together, these measures should further accelerate the security clearance process so that all firms – but especially critical infrastructure organizations – can better protect themselves and the country against cyber threats.

Adoption of the Framework should enhance the value of holding a security clearance because firms that satisfy its requirements will be in a better position to leverage threat information and protect their own systems in a more timely and effective manner. As a result, there will be increasing pressure on the federal government to eliminate bottlenecks and process security clearance applications as quickly as possible. Treasury believes the above measures should further accelerate the process, and because they are administrative actions, would not require additional legislation.

* * * * *

All five of these policy options are worthwhile in and of themselves, even if their implementation is not made contingent on Framework adoption. But policymakers will face a clear trade-off as they determine whether or not to implement them as incentives for adopting the Framework. If they are used as incentives, they may have a more narrow effect by encouraging additional critical infrastructure organizations to adopt the Framework. If they are not made

conditional on adoption of the Framework, then these policy options could benefit a broader array of firms.

Based on its current analysis, Treasury has identified two policy options that do not warrant further consideration as a government-provided incentive to encourage critical infrastructure organizations to adopt the Framework.

Tax Incentives

Tax incentives could encourage additional cybersecurity research as well as additional critical infrastructure investment in cybersecurity assets, whether through tax credits or accelerated cost recovery deductions. Certain tax incentives, while currently not targeted at cybersecurity activities, nevertheless may apply to research and other investments. However, additional legislation would be required to expand those incentives specifically for cybersecurity activities. Although several critical infrastructure stakeholders suggested tax incentives might encourage firms to adopt the Framework, tax incentives are difficult to target specifically at cybersecurity activities, and harder still to target at cybersecurity investments that firms would not otherwise make. Ultimately, adoption of a tax incentive would come at the expense of foregone revenue for the government or reallocation of existing fiscal obligations. ***Accordingly, Treasury does not recommend further consideration of tax incentives at this time.***

Cyber Insurance

Cyber insurance could cause critical infrastructure policyholders to bolster cybersecurity since insurers have strong financial incentives to establish minimum-security standards, monitor cyber threats, and improve the quality of data collection. However, cyber insurance is a growing but nascent industry. Direct government involvement may not be necessary and could, in fact, impede the development of a private market. Nevertheless, the natural development of the private cyber insurance market could advance cybersecurity, and through its standard-setting and compliance functions, may indirectly spur adoption of the Framework. The Framework may also encourage the growth of the private cyber insurance market to the extent that it establishes minimum standards for the cyber insurance industry. That is why significant input and collaboration with the insurance sector could play a critical role in determining the success of the Framework.

No additional legislation would be needed for the continued development of the private cyber insurance industry. ***Accordingly, Treasury does not recommend the creation of a government program for cyber insurance at this time.***

Click HERE to read Treasury's Supporting Analysis for this report.