

White House and Department of Homeland Security (DHS) Float Incentives for Adopting Cybersecurity Framework

Article By:

Litigation Practice Group Schiff Hardin

On August 6, 2013, an article titled “Incentives to Support Adoption of Cybersecurity Framework” was posted on both the [White House blog](#) and on the [Department of Homeland Security \(DHS\) Web page](#). In this article, the Administration appears to be suggesting ways federal agencies and Congress may create incentives for the adoption of a voluntary Cybersecurity Framework that is currently under development by the National Institute for Standards and Technology (NIST).

As we reported in February in two blog posts (“[President Obama Issues Executive Order — Improving Critical Infrastructure Cybersecurity](#)” on February 15, 2013 and “[The Cybersecurity Executive Order’s Effect on the Electric Industry](#)” on February 21, 2013), President Obama issued Executive Order No. 13636 to improve cybersecurity in the energy industry and across all other critical infrastructure sectors. Under that executive order, NIST was tasked with developing a Cybersecurity Framework that shall include “standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks.” NIST will be releasing a preliminary Cybersecurity Framework in October 2013 and a final version is due in February 2014.

Executive Order No. 13636 made clear that this Cybersecurity Framework would be voluntary, but the President directed the Secretaries of DHS, Treasury and Commerce to establish a set of incentives to promote participation in the program by private industry. As reflected in the White House and DHS blog posts, the three departments have conferred, solicited comments, and have provided to the President recommendations on these incentives. These recommendations include asking federal agencies and Congress to explore incentives in the following eight areas:

- Cybersecurity insurance – Engaging the insurance industry to build underwriting practices to promote adoption of the Cybersecurity Framework and foster a competitive cyber insurance market
- Grants – establishing participation in, or adoption of, the Cybersecurity Framework as a condition of or one of the weighting criteria for federal critical infrastructure grants
- Process Preference – Expediting existing government process delivery (other than incident response) for participants in the voluntary program

- Liability Limitation – Developing information to provide to Congress to consider regarding “reduced tort liability, limited indemnity, higher burdens of proof or the creation of Federal legal privilege that preempts State disclosure requirements” to encourage participation in the voluntary program
- Streamline Regulations – Exploring the interaction of the Cybersecurity Framework and existing regulations to help make compliance easier
- Public Recognition – Exploring the efficacy of providing optional public recognition for participants in the voluntary program and their vendors
- Rate Recovery for Price Regulated Industries — Encouraging further dialogue with federal, state and local regulators and sector-specific agencies on considering allowing utilities recovery of cybersecurity investments related to complying with the Cybersecurity Framework
- Cybersecurity Research – Identifying areas where commercial solutions are available to implement the Cybersecurity Framework and gaps where those solutions do not currently exist

The incentives article makes clear that these recommendations do not reflect final Administration policy and that agencies are to examine these recommendations over the next several months. In the case of Liability Limitations and Rate Recovery, it is clear that the Administration will need to work with Congress and/or state and local governments to develop formal incentives for industries. DHS, Treasury and Commerce are working with “appropriate agencies” to prioritize each incentive and move forward.

© 2025 ArentFox Schiff LLP

National Law Review, Volume III, Number 221

Source URL: <https://natlawreview.com/article/white-house-and-department-homeland-security-dhs-float-incentives-adopting-cybersecu>