Member Perspectives on Incentives

Incentives

Comments were offered on the following incentives proposed by the Integrated Task Force for the Implementation of the EO and PPD-21:

Grants are an effective means for encouraging adoption of a cybersecurity framework.

Direct Federal funding for investment in the framework would be beneficial.

It is important to clearly articulate any contingencies associated with the grants.

Funding results should be outcome-based, and penalties should not exceed the value of the grant.

Grants should be focused on creating capability that can benefit an entire industry sector, and not one company, i.e. industry training programs, information sharing capability, research consortium for sector specific technologies, etc.

Liability caps are more effective than liability reductions.

Security is not improved by simply transferring risk to insurance companies. A more effective strategy for encouraging participation would be to cap the liability associated with compliance with the cybersecurity framework.

Not capping liability may create an environment in which insurance underwriters dictate security policy.

Companies acting in good faith should not see additional risk in adoption of the framework.

A policy similar to the SAFETY Act, which provides liability protection to encourage adoption of the "Cybersecurity Framework" or similar industry standard, should be considered as an option.

The Federal Government should require cybersecurity framework compliance on its suppliers, related to critical infrastructure.

Government procurement power has numerous indirect benefits for the private sector. It incentivizes suppliers to enhance the security of their products and services — which are often the same products and services used in private critical infrastructure.

The Government needs to include hardware and software suppliers in any scope of procurement policy. Reducing the risk associated with hardware and software systems allows owners and operators to redirect their attention to other critical security concerns.

Many risks that CIKR owners/operators face are a direct result of vulnerabilities within purchased IT hardware and software.

Evaluation and leveraging of existing regulations

Leveraging of compliance with existing laws into the framework is more effective than introducing new rules that may create conflict.

Many cybersecurity policy and practices are already regulated.

Layering additional policies and regulations on top of current regulations will create larger compliance models reducing flexibility, increase costs, and reduce effectiveness.

Two additional incentives were suggested in comments:

A robust, dynamic risk identification process

Compliance with the cybersecurity framework compliance needs to be focused on the major risks in critical infrastructure.

Greater credibility will be granted to a program that allows an owner/operator to focus adoption on the major risk areas. It will emphasize protection of vital assets, as well as reducing cost to both industry and the Federal Government.

Rate recovery for price regulated industry is an effective incentive; however, keeping the focus on high risks lowers downstream consumer impact.

Ensuring the availability of qualified, vetted security professionals

New areas of compliance require additional professionals to ensure compliance, and qualified personnel can be challenging to find.

Federal assistance with background checks, and leveraging of existing programs could establish a greater reserve of qualified professionals.

Place a focused emphasis on training, as referenced in the NIAC's 2006 report on Workforce Preparation, Education and Research. In that report, the NIAC noted several areas in which training could be improved. These included:

- Studying high-achieving international competitors to establish competitive teaching and curricula standards
- Expanding internship and employment options to include critical infrastructure owners and operators and government contractors performing specific, documented intelligence analysis tasks for Federal, State, and local governments
- Lessening the challenge of obtaining a security clearance for graduates

- Increasing and stabilizing funding for fundamental research in unclassified cybersecurity
- Developing and maintaining standardized intelligence analysis position descriptions, for all Federal agencies, in order to provide an overview of the knowledge, skills, and abilities necessary for the tasks
- Designating a privately administered, public-private intelligence analysis training certification body

In 2008, the NIAC, in its report titled "The Insider Threat to Critical Infrastructures," also addressed the issue of vetting security professionals. In the Employee Screening section of the document, the Council noted that critical infrastructure owners and operators need access to fingerprint-based Federal and State criminal history records as a means of enhancing insider threat risk assessment, and recommended that Congress provide owner/operators with the ability to access this information. The Council also recommended including funding for improving the accuracy and standardization of records; standardizing records; funding development of a program to educate users on reading RAP sheets; and conducting checks of State employment records where possible, and Federal records in other instances. The NIAC also recommended acknowledging the diversity of the size and resources of owner/operators by allowing discretion on when to participate and screen employees; establish their own adjudication criteria to meet differing levels and types of risk; and to screen current and prospective employees on an as-needed basis.

Anti-trust protection

The effectiveness of the Executive Order and subsequent PPD relies heavily on the sharing of threat information between the public and private sectors, but also will require sharing amongst private sector companies. Currently this sharing is discouraged due to the concern of violating, or the appearance of violating, of Anti-Trust regulations. Government must provide Limited Anti-Trust vehicles that provide protections for companies that discuss and share cyber threat information.

The NIAC previously noted the value of limited antitrust protections in its 2009 report, titled "Critical Infrastructure Resilience," in relation to the Protected Critical Infrastructure Information (PCII) program. In that report, it was noted that the United Kingdom has enhanced risk information sharing among competitors by scrubbing the source of the information, and focusing only on mitigation methods, and that a similar set of rules could dispel fears of using such information against the entity providing it.