Overview

Presidential Executive Order (EO) 13800 - *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, required the Secretary of the Department of Homeland Security (DHS), in coordination with the Secretary of Commerce to provide a report to the President by August 9, 2017 that examines the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cybersecurity risk management practices, with a focus on publicly traded critical infrastructure entities.

The report was developed through a collaborative interagency process. Due to the 90-day timeframe prescribed, the report focused on the identification of existing Federal policies and practices; identification and review of third-party evaluations of transparency practices and systems from independent sources; and limited private industry engagement available in the short-timeframe. DHS conducted a literature review of secondary sources addressing the sufficiency of existing Federal policies and practices in promoting transparency of cybersecurity risks and risk management practices, and the effectiveness of transparency systems, in general, in advancing policy goals. There were 96 different sources identified as part of the literature review, and several Federal policies and practices identified. While no formal tasking resulted from the development of this report, the associated findings provide insight into the effectiveness of transparency systems; the sufficiency of existing Federal policies and practices; and informs future policy discussions regarding market transparency and improving cybersecurity outcomes.

Effectiveness of Transparency Systems

Transparency systems in general. Beginning with transparency systems in general, the literature reviewed finds that of the various forms of transparency systems, *those that embed information into the decision processes of both information users and disclosers are highly effective*. These transparency systems, such as corporate financial disclosure, restaurant hygiene quality cards, and mortgage lending reporting, are highly effective in that they lead to consumers obtaining relevant, disclosed information and then enables making choices that lead disclosers to alter their behavior and make behavior more congruent with policy intentions. For example, corporate financial disclosure leads to institutional and individual investors using key indicators from quarterly and annual reports to inform stock purchases and sales. Company managers, in turn, track investor responses to their financial disclosures as a routine practice and respond to perceived investor concerns.
Cybersecurity transparency systems. Moving more specifically to cybersecurity transparency systems, the identified Federal policies and practices spanned all critical infrastructure sectors, with sector-specific policies in the Communications; Energy; Financial Services; Healthcare and Public Health; and Nuclear Reactors, Materials, and Waste sectors. The review of current and existing policies reveal that although some progress has been made in recent years, limitations remain and there is much to be done to improve transparency in cybersecurity risk management. The questions raised below will inform future policy considerations.

Suggestions for Further Research and Policy Considerations

The examination of the sufficiency of existing federal policies and practices identified a number of questions that warrant further research and policy considerations, including:

1. Can publicly-traded companies disclose meaningful information to investors without providing information that would be useful to adversaries?

2. Can federal policies and practices guide critical infrastructure entities in finding a balance between disclosing meaningful information that promotes transparency of cybersecurity risks and risk management practices without disclosing information that could be useful to adversaries?

3. What is the correlation between disclosure (or lack thereof) and cybersecurity breaches in publicly traded companies?

4. How can existing potential disclosure policies help foster efficient investment in security without the need for further regulation?

5. How can government initiatives and public-private partnerships support effective understanding and communication of risk-reducing investments?

6. Independent of federal policies and practices, to what extent do incentives exist to encourage critical infrastructure entities to be transparent about cybersecurity risks and risk management practices? To what degree do such incentives have the potential for promoting cybersecurity risk management among these entities?

7. To what degree do critical infrastructure entities have effective means for providing input to the federal government on its policies and practices, through membership on steering committees, in councils, as part of public-private partnerships, and through other channels? How might this type of engagement by critical infrastructure entities encourage these entities to become more transparent about cybersecurity risk and risk management practices?

8. Do market practices other than required public disclosure – such as due diligence, insurance underwriting, or corporate auditing – support appropriate transparency in the marketplace regarding cybersecurity risk and risk management practices?

9. How does reporting cyber incidents to, and cooperating with, law enforcement promote market transparency, and how can federal policies and practices encourage reporting of cybersecurity incidents to appropriate law enforcement authorities?
Reference List


