By Executive Order: Delivery of Cyber Intelligence Imparts Cyber Responsibilities

Roland L. Trope
Trope and Schramm LLP

Stephen J. Humes
Holland & Knight

The US, like most countries, is grappling with how to handle cybersecurity issues, especially threats to critical infrastructure. How and where should a government intervene, and which entities have responsibility for notice and action? In this special report, we invited Roland L. Trope and Stephen J. Humes to comment on a recent US Executive Order and its evolution from failed attempts to enact cybersecurity legislation. Although the details are specific to the US, the lessons are applicable to everyone. —Shari Lawrence Pfleeger, editor in chief

This article explores a new Executive Order (EO) entitled “Improving Critical Infrastructure Cybersecurity” and the unsuspected burdens it places on companies it seeks to assist (www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity). The EO authorizes dissemination of cyber intelligence reports to owners and operators of certain enterprises. It also directs the collaborative development and implementation of risk-based cybersecurity standards. Here, we examine the provisions for sharing cyber intelligence reports and illuminate what they leave unsaid—that each report delivered will create cybersecurity responsibilities for its recipients. Our purpose is to help business owners and operators prepare for the consequences that this creates: a brave new world in which company recipients of cyber intelligence reports discover that such reports add to their uncertainties by imparting corporate cyber responsibilities.

Background

The EO aims to enhance the cybersecurity of “critical infrastructure” enterprises, defining the term to mean “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” Examples include major electricity generation, transmission, or distribution enterprises; financial institutions; and transportation providers.

Over the past decade, this country’s critical infrastructure enterprises have increasingly experienced not only random infections by malware, but also damaging intrusions from cross-border, persistent cyberattacks aimed at predetermined targets. Post-attack analyses cautioned that potentially catastrophic long-term damage might result unless a national cybersecurity strategy emerged (www.ft.com/intl/cms/s/0/989a68c-692e-11e2-b254-00144feab49a.html#axzz2Jx72tVWH). Without a national plan, the strategy for critical infrastructure enterprises remained fragmentary, incomplete, and of uncertain reliability; it probably would not ensure that enterprises could defend against, minimize the effects of, or restore degraded capabilities after a damaging targeted cyberattack.

In 2012, senior military and intelligence officials urged, with some Congressional support, “immediate action on cybersecurity legislation” (http://commerce.senate.gov/public/?a=Files.Serve&File_id=b0229d56-1881-4ee2-8934-fb474d9dd6b2). Although introduced, the Cybersecurity Act of 2012 did not pass: the US Chamber of Commerce “strenuously opposed” it, instigating a Senate filibuster that blocked the bill in August (http://articles.latimes.com/2012/aug/03/nation/la
companies prompted a rethink of the need for government intervention.”

Nonetheless, in February 2013, a White House senior director for cybersecurity cautioned “an executive order is not magical. … It doesn’t create new power or authorities for any government agency. … [I]t’s an expression of the president’s strategic intent. … not a substitute for legislation” (http://thehill.com/blogs/hillicon-valley/technology/281477-white-house-cyber-official-executive-order-is-not-magical-and-cyber-bill-is-needed). Finally, on 12 February 2013, President Obama signed the EO and declared his cyber concerns during his State of the Union Address that night.

**Strategic Incentives**

The EO aims to coax companies to improve their capabilities to withstand a serious cyberattack, to limit the damage it might cause them and others that depend on them, and to restore disrupted operations as soon as practicable. Most companies have been reluctant and slow to make such efforts a high priority, and some have yet to take cyberthreats seriously. To change company attitudes and policies, the EO pointedly addresses its initiatives to company policy makers—owners and operators—and offers them positive and negative incentives, what we’ll refer to as carrots and sticks. But first, it sets the stage by seeking to impress on everyone the urgency of taking cyberthreats seriously. The EO therefore opens with what amounts to a national cyber risk assessment:

> Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.

The EO authorizes several concurrent strategies to defend critical infrastructure against damaging cyber intrusions. Some of the strategies focus on voluntary measures. They aim at creating incentives, or carrots, to encourage owners and operators to enhance their enterprises’ cybersecurity (consistent with efforts expressly required to minimize or mitigate the privacy and civil liberty risks that such measures might create). The carrots include the following:

- expanding participation in the Enhanced Cybersecurity Services (ECS) program,

In mid-November, the Senate declined again to act when, by a 51-47 vote, it defeated a procedural motion to move forward, which killed the bill. The White House continued to develop the draft Order. A revised "Predecisional / Deliberative" draft, dated 21 November 2012, began to circulate. Concurrently, some industries that had opposed legislation became more receptive, “after unprecedented cyber attacks against financial institutions and energy companies prompted a rethink of the need for
to let businesses share indicators of malicious cyberactivity not only with providers of Internet, network, and communications services but with “all critical infrastructure sectors” ([https://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf](https://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf));

- increasing the information shared through the ECS program to include “classified cyber threat and technical information,” but only to a subset of participants—namely, the “eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure”;
- directing the National Institute of Standards and Technology to coordinate development of a “Cybersecurity Framework,” a set of “voluntary consensus-based standards and industry best practices to the fullest extent possible” to help owners and operators of critical infrastructure “identify, assess, and manage cyber risks;” and
- directing the DHS Secretary to establish a voluntary program to support adoption of the Cybersecurity Framework, seeking to identify and establish incentives for critical infrastructure owners and operators to participate in the Framework and adopt its cybersecurity standards, but conditioning the establishment of incentives on whether they would “require legislation or can be provided under existing law and authorities to participants” in the Framework program.

Among its carrots, the EO tucks some sticks, some of which appear at first glance to resemble carrots. They give industry what it has often requested: access to federal cyberthreat intel reports. Let’s look more closely at two kinds of intel the EO will give to owners and operators.

**Imminent Target Notices**

One kind of intel will be “unclassified reports of cyber threats to the US homeland that identify a specific targeted entity.” A process will be developed that rapidly disseminates these reports to the “targeted entity.” The process will also disseminate “classified reports to critical infrastructure entities authorized to receive them.” Looks like a carrot.

But we can’t help thinking that lurking inside it is a stick. Here’s why. Consider what it means to receive such information—it puts owners and operators on notice that their companies are the threat’s predetermined targets (let’s call these Imminent Target Notices). If you’re an owner or operator, a director or officer, and the government alerts you that your company’s a target, it’s probably going to be hard to avoid asking yourself, your executive management team, your board, and your counsel a battery of questions: “We can’t ignore this, can we? Does this trigger any disclosure or reporting obligations? Do stockholders have the right to know this company has been identified a target so they can make informed investing decisions? What should we be doing before we’re attacked? Shouldn’t we reexamine our cyber defenses and disaster recovery plans? If we don’t, and we’re severely damaged and slow to restore operations (as after super-storm Sandy), it will drive up the recovery costs, tank our reputation, and hammer the company’s valuation. If our customers, suppliers, and stockholders learn that we had warning and didn’t prepare to limit damage and recover quickly, they’ll blame us for their losses—direct or collateral—and they’ll sue us.”

The closer we look at the EO, the more inevitable it seems that some courts will view receipt of information in an Imminent Target Notice as imposing on owners and operators, officers and directors, a duty to fulfill certain corporate cyber responsibilities.

Such courts might impose liability by drawing an analogy to a famous case in which barges towed by tugs sank in a gale. Barge owners sued tug owners, alleging the tugs were unseaworthy because they didn’t carry a new, widely available technology—radio receivers. They therefore couldn’t receive warnings of deteriorating weather. The court not only held the tug owners liable but emphasized that “there are precautions so imperative that even their universal disregard will not excuse their omission” ([The T.J. Hooper v. Northern Barge Corporation, 1932](https://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf)). A recent case reiterates the point in the cyber era: “there are circumstances in which the nature and likelihood of a foreseeable security breach and its consequences will require heightened precautions” ([Nash v. The Port Authority of New York and New Jersey, 2008](https://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf)).

The EO encourages this view by declaring it the policy of the US government “to increase the volume, timeliness, and quality of cyber threat information shared” with private-sector entities so that they “may better protect and defend themselves against cyber threats.” Moreover, the
cleared companies, those authorized to receive classified intel reports, will be under an even heavier burden to use them to protect and defend themselves against cyberthreats. They must also ensure adversaries don’t access these reports. Whether a cyberattack reveals that a company has failed to fulfill such cyber responsibilities will probably be decided by courts. And whereas Congressionally enacted statutes can grant immunity from liability for companies that comply with federal cybersecurity standards, Executive Orders cannot.

Once grasped, that’s no carrot. And in the hands of companies and people harmed by the avoidable consequences of a foreseeable cyberattack (confirmed by the government’s warning), it’s a stick that will threaten like a cudgel.

**Catastrophic Target Notices**

The EO also authorizes what we call Catastrophic Target Notices, which do not report a threat but identify critical infrastructure “where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.” Catastrophic Target Notices will confidentially notify owners and operators that their companies have been so identified and provide them with the basis for that determination.

Recipients of Catastrophic Target Notices will almost certainly start to ask themselves, their board, and their counsel questions similar to recipients of Imminent Target Notices but with the added burden that if they don’t make every reasonable effort to minimize the ripples of damage beyond their company, a cyberattack on their assets will harm other enterprises, employees, investors, suppliers, and customers. Granted, a Catastrophic Target Notice should rarely come as a surprise (especially to owners and operators of critical infrastructure in regulated industries). But it nonetheless magnifies owners’ and operators’ responsibilities by raising the stakes for failures to address cybersecurity adequately. Notice recipients might quickly realize that they don’t want that burden and begin steps to avert catastrophic damage regionally and nationally.

**Forewarned, Forearmed**

It’s little consolation that the EO gives you a chance of escaping this imposed “identity.” There will be a process for companies to “submit relevant information and request reconsideration” by the DHS of their identification as a catastrophic target. Consider, however, the costs of assembling evidence, expert testimony, and legal arguments to overcome a DHS determination based on classified intel.

In the meantime, recipients must come to terms with the possibility that the DHS has imposed on owners and operators, directors and officers, a set of undefined, ambiguous but possibly extraordinary corporate cyber responsibilities. Imagine a specter of burgeoning liability that could attach to your company or its board if a cyberattack strikes and demonstrates the accuracy of the DHS’s warning of catastrophic regional or national damage. Cyber insurance policies might start excluding from coverage recipients of DHS notices or condition coverage on steeply priced premiums. This isn’t a carrot—it’s a big stick.

Moreover, your company won’t want to disclose to outsiders that it received an Imminent Target or Catastrophic Target Notice. Tell a customer, and it might prudently shift its business to a less risky seller. Tell a supplier, and it might demand shorter, tighter payment terms. Tell stockholders or investors, and they might elect to divest. If you receive both kinds of notices, these problems could grow prodigiously, and addressing them will need to be expedited, which will further increase the company’s cyber safeguard costs.

Meanwhile, within the company, efforts to address the corporate cyber responsibilities bestowed by the DHS’s notices might be hindered by what the notices don’t provide. For example, the EO doesn’t provide for expiration of the notices, leaving owners and operators to speculate when, if ever, they might be relieved of these corporate cyber responsibilities. A publicly owned company will need to decide whether it can keep receipt of DHS notices a company secret or must disclose it to investors in a US Securities and Exchange Commission (SEC) filing (to comply with the SEC Staff’s Guidance on Cybersecurity disclosures; [www.sec.gov/divisions/corpfin/guidance/cfguida nce-topic2.htm](http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm)).

Thus, the strategy implicit in the EO’s use of notices is the proverbial “forewarned — forearmed.” Receipt of a notice will narrow owner-operator alternatives. Inaction is unjustifiable; superficial action, when viewed by judges, risks being deemed negligent or recklessly indifferent to clear government
warnings. Notices will make it difficult to excuse postponing investments in cybersecurity and disaster recovery as courts might view receipt of a notice as putting the onus on owners and operators to justify what they subsequently did and did not do. If a head-in-the-sand approach to cybersecurity prevailed at a company, that approach will probably be relinquished upon delivery of DHS notices.

Receipt of DHS notices also requires preparation. Companies should examine Presidential Policy Directive/PPD 21, issued with the EO (www.fas.org/irp/offdocs/pdd/ppd-21.pdf). PPD 21 sheds light on steps the EO expects (but cannot require) owners and operators to take. Specifically, it adds to cyber “security” the concept of “resilience,” which it defines as “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.” A DHS notice should put companies on notice to reinforce their resilience to cyberattacks, and to develop capabilities for situational awareness during and after an attack.

The EO purports to achieve its goals “through a partnership with the owners and operators of critical infrastructure.” Close analysis reveals a subtler modus operandi: it offers incentives to owners and operators of all companies to adopt voluntary standards and improve their cybersecurity. But we doubt the White House really expects that such incentives, without enforcement, will overcome the inertia of companies that haven’t experienced severe cyberattacks or that are not federally regulated critical infrastructure enterprises. The power of the EO rests with its notice provisions. By authorizing the DHS to issue Imminent Target and Catastrophic Target Notices, the EO will create a special class of company owners and operators upon whom each DHS notice will confer the burdens of corporate cyber responsibilities. By sharing its intel with owners and operators, the government pressures them to act quickly, diligently, and with an eye to the possibility that a court will be asked if they made a reasonable investment to fulfill their responsibilities. The uncertainty of the court’s view and the indeterminate size of potential liability will impress them, thereby persuading many to invest in preparations they might have repeatedly deferred making or been reluctant to make so expansively.

No owner or operator can refuse to accept a DHS notice or remain inattentive or unresponsive to it. Each recipient will probably sense that it (and other recipients) now has what no other companies have—duties to fulfill unspecified, undeniable, and potentially far-reaching corporate cyber responsibilities. Owners and operators will need to address that issue quickly. If they believe they have such responsibilities, they’ll need to determine what actions they should prudently take to protect their company from the potentially staggering liability that they could be exposed to in the event of a cyberattack, if in hindsight they’re viewed as having failed to do what they reasonably should have done. Courts measure such failings by standards of foreseeability. DHS notices might raise the applicable standard by changing the foreseeable into a federal forecast based on expert analyses of classified cyberthreat intel. Owners and operators, particularly of critical infrastructure enterprises, should imagine receiving DHS notices and, having glimpsed the future, start preparing to cope with the burdens of this new “partnership.”

Acknowledgments
We thank Sarah Jane Hughes, Michael Fleming, John D. Gregory, Candace Jones, Miggie Cramblit, George Winborne, and Winston L. Trope for their constructive criticisms, suggestions, and assistance in editing the manuscript. The views expressed herein are the personal views of the authors and have not been reviewed or approved by, and should not be attributed to, the US Military Academy, the Department of the Army, the Department of Defense, or the US government.

Reference

Roland L. Trope is a partner at Trope and Schramm LLP in its New York City office; adjunct professor in the Department of Law, US Military Academy at West Point; and a member of the ABA Task Force on Cybersecurity. Contact him at rltrope@tropelaw.com.

Stephen J. Humes is a partner at Holland & Knight in its New York City office and a member of the ABA Section of Environment, Energy, and Resources. Contact him at Steve.Humes@hklaw.com.