LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Information Law, Data Privacy & Cybersecurity Practice

May 18, 2017 | Number 2143

New Executive Order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"

Trump Administration's required cybersecurity assessments provide potential for new round of public-private collaboration.

The Trump Administration recently issued a much anticipated Executive Order (EO) addressing cybersecurity, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (May 11, 2017). It directs federal executive agency heads to undertake various cybersecurity-related reviews and to report findings back to the White House within prescribed timetables ranging from 60 days to one year. The same week saw a successful large-scale ransomware attack affecting thousands of organizations across many countries, underscoring the vulnerability of individuals, businesses and governments on a digitally connected planet.

Unlike some of the Trump Administration's recent executive orders, the new cybersecurity EO does not aim to unwind policies put in place or initiatives undertaken by the Obama Administration. Rather, subsequent steps by the Trump Administration following the new EO will likely build upon the previous Administration's efforts. But while this latest EO does not mark a substantial policy shift, it does provide a useful catalyst for a new round of engagement between private-sector owners and operators of critical infrastructure and the current Administration. Some of the previous Administration's cyber initiatives had appeared to be losing momentum in the new Administration; the Trump EO now commits the new Administration to a cybersecurity agenda.

This *Client Alert* first provides a brief summary of the new EO, contextualized against the backdrop of the previous Administration's efforts. It then identifies some of the issues addressed in the EO that call for private-sector engagement. While the new EO addresses cybersecurity and critical infrastructure generally, it also highlights the importance of cyber resilience of the electrical power system in particular. This *Client Alert* focuses especially on the power sector and grid security.

The Threat

The basic threat to which the new EO responds is well-understood. As malicious cyber tools have become less expensive and increasingly available sophisticated cyber disruptions, attacks, and malicious information-gathering are undertaken by actors far below the nation-state level. Monitoring cyber adversaries and potential adversaries becomes more difficult with their proliferation and meanwhile potential points of entry into cyber networks have multiplied with the internet of things. Thus the central challenge of cybersecurity: to prevent proliferating adversaries in possession of evolving tools from malfeasance over an increasing number of possible access points.

The cybersecurity of the nation's electric grid illustrates. The electrical grid is foundational not only to the daily operation of the nation's economy but also to its national defense, given that much economic activity as well as the country's military capabilities presuppose a reliable electrical system. Yet a number of factors — the expansion of the grid, deregulation of power markets accommodating more market participants, automation and other innovations to improve electrical system performance, distributed generation, smart meters and smart homes — increase the potential risks of cyber events that could disrupt portions of the electrical system. Similar developments likewise increase the risks of cyber compromise for power generators and others connected to the grid, which face cyber threats from malware infiltration, insider threats and supply-chain risks, among other vectors. And whereas the government holds more or less exclusive control over the tools (offensive, defensive and informational) that protect the nation from attack by air or by sea, cyber protection of the electrical system inherently requires collaboration between the government and private entities that own critical energy infrastructure assets.

The Trump Executive Order

The new EO calls for assessments of the nation's cybersecurity systems, falling into three categories.

***Cybersecurity of Federal Networks*.** The Trump EO first emphasizes cyber threats to the federal government's own networks, tasking federal agency heads to assess cyber risks, to adopt risk management measures to address those risks and to report on their management of cyber risks to federal networks. Section 1 furthermore tasks the Secretary of Homeland Security and the Director of the Office of Management and Budget, together with the Secretary of Commerce and the Administrator of the General Services Administration, to review agency reports and submit their assessment of agencies' mitigation measures to the White House along with a plan for addressing unmet agency needs and reconciling agency practices. With respect to federal networks implicating the national security system in particular, the EO directs the Secretary of Defense and the Director of National Intelligence to manage federal network risks and to report to the White House on their implementation of risk-mitigation practices.

Cybersecurity of Critical Infrastructure. The EO next addresses cyber risk management by "the owners and operators of the Nation's critical infrastructure." The EO tasks the Secretary of Homeland Security — "in coordination with" with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the FBI and the heads of other agencies that work closely with sectors that comprise the country's critical infrastructure — to identify authorities and capabilities that could be employed to support the cybersecurity of critical infrastructure, and to report to the White House concerning how those resources should be used and identifying any obstacles to their best use. Section 2 also directs the Secretary of Defense, together with the Secretary of Homeland Security, the FBI Director and the Director of the Office of National Intelligence to provide a report concerning cybersecurity risks facing the nation's military and defense systems and networks with recommendations for how to mitigate those risks.

***Cybersecurity for the Nation*.** Finally, the EO addresses the cybersecurity of the American people more generally. Like Sections 1 and 2, Section 3 calls upon executive branch leaders to assess strategic options for protecting citizens from cyber threats, including fraud and theft. It also requires assessment and a report to the White House concerning the strength of international cooperation against cyber threats, recognizing that the nation is "dependent on a globally secure and resilient internet and must work with allies and other partners." The EO also calls for an assessment of the sufficiency of education and training in the United States "for the cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education."

The new EO is noteworthy also for what it does not do. It neither supplants nor unwinds the previous Administration's efforts in this arena, perhaps not surprisingly in light the substantial work and public-private collaboration already undertaken by the previous Administration. Rather, the new EO's provisions concerning critical infrastructure explicitly reference both Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (February 12, 2013) and Presidential Policy Directive 21 addressing "Critical Infrastructure Security and Resilience" issued on the same day. EO 12636 and PPD 21 together set in motion a number of cybersecurity initiatives across the executive branch and focused on particular sectors relevant to the nation's critical infrastructure.

One such initiative was the National Institute of Science and Technology's (NIST's) development of a "Cybersecurity Framework." Executive Order 13636 required NIST to create a Cybersecurity Framework — consisting of "standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks" and reflecting consensus standards and industry best practices across different sectors including the owners and operators of critical infrastructure."[1] The new Trump EO requires federal agency heads to use the NIST's Cyber Framework "or any successor document" to manage agencies' cyber risks.

For another important example, Section 2(e) of the new EO addresses threats to the electrical grid, calling for an assessment of the ability of the nation's power system to respond to a "significant cyber incident" as that term is defined in President Obama's Presidential Policy Directive 41 concerning "United States Cyber Incident Coordination" (July 26, 2016). PPD 41 built upon EO 13636 and PPD 21 by further enhancing federal coordination and planning for cyber incident response, including increased centralized coordination among "sector specific" federal agencies, that is, agencies assigned primary responsibility for specific sectors of the economy by PPD 21 and tasked by both EO 12636 and PPD 41.[2] The new Trump EO calls for the Secretary of Energy, in consultation with the Director of National Intelligence and others, to assess the potential scope and duration of a prolonged power outage resulting from a cyber attack, as well as the readiness of the country "to manage the consequences of such an incident" and also to identify "any gaps or shortcoming in assets or capabilities required to mitigate the consequences of such an incident."[3] The Energy Secretary is to do so as the head of the "sector specific agency" for the energy sector as designated earlier by PPD 21.

Electricity Sector Coordination in the Previous Administration

PPD 21 had already charged the Department of Energy to work with the energy sector to strengthen the security and resilience of critical energy infrastructure, to serve as the day-to-day federal interface for coordination with the energy sector, to carry out cyber incident management, and to provide support and assistance to the energy sector to identify risks and mitigate incidents. One form that coordination took was the Electricity Subsector Coordinating Council (ESCC), a public-private effort co-led by the Department of Energy and leaders of the electricity sector, including utility CEOs, to coordinate preparation and response to critical infrastructure, including cyber risks.[4] For another example, the Critical Risk Information Sharing Program (CRISP) launched in 2013 provides two-directional sharing between government and industry of cyber threat data, as well as information that may be actionable and how to mitigate cyber threats.[5] Here too, companies from the electricity sector (representing more than 75% of US electricity customers) participate in CRISP, with the North American Electric Reliability Corporation (NERC) providing additional leadership. NERC also oversees the Electricity Information Sharing and Analysis Center (E-ISAC), the mission of which is to reduce physical and cybersecurity risks to the electricity industry.[6] E-ISAC works collaboratively with DOE and with the ESCC to prepare for and respond to cyber threats and incidents. Such collaborations began to merge increasingly during the final year or so of the Obama Administration. As explained below, they are likely to provide the organizational architecture for additional initiatives by the Trump Administration following from the new EO.

The FAST Act and Cyber Attacks Against Critical Infrastructure

Congress also addressed cybersecurity of the electrical system with passage of the Fix America's Surface Transportation Act (FAST Act) in December 2015. While much of the FAST Act addressed authorities and appropriations concerning the Department of Transportation, it also expanded the Secretary of Energy's authority to address threats to the electricity supply — an authority centrally relevant to the assessment the Secretary of Energy is to provide under the new cyber EO.

Specifically, the FAST Act included a provision added to the Federal Power Act, Section 215A, which gives the Secretary of Energy authority to issue orders as remedial measures in response to a "grid security emergency."[7] In contrast to the Secretary of Energy's emergency authorities as they existed before the FAST Act — enabling DOE to address emergencies arising variously from severe storms, power shortages, and fuel shortages for example — the new provision is triggered by much more narrow circumstances; an imminent or actual grid security emergency defined as a "malicious act using electronic communication or an electromagnetic pulse" or a "geomagnetic storm event" that disrupts devices of communication networks essential to the grid's reliability.[8] But once triggered, this new authority broadly allows the Secretary of Energy to issue any temporary order "necessary in the judgment of the Secretary to protect or restore" the grid,[9] although the statute calls for consultation with industry — naming the ESCC specifically — "to the extent practicable" given the exigencies of an emergency.[10]

The FAST Act also required DOE and the Federal Energy Regulatory Commission to undertake certain rulemakings concerning critical electric infrastructure that implicate the interests of power generators and transmission operators (among others stakeholders). In particular, FERC was charged to develop a procedure by which entities subject to emergency orders could submit claims for compensation, to the extent those subject to orders would bear additional unrecoverable costs as a result,[11] as well as to delineate a new exception to the Freedom of Information Act for "critical electrical infrastructure information."[12] The Department of Energy was charged by the FAST Act to issue a procedural rule explaining how the Energy Secretary's new authority will be exercised, for example with respect to any prior notice of remedial measures, how parties subject to an emergency will have to demonstrate compliance, possible requirements for clarification or reconsideration of such an order, and so on.[13] This latter rulemaking was well underway during the final months of the Obama Administration, but as of this writing has not been finalized.

Potential Next Steps and Opportunities for Private Sector Participation

The new Trump EO presents a fresh round of opportunity for the private sector to engage further with the federal government concerning cybersecurity and resilience, through the initiatives identified above and perhaps beyond.

First, private parties will likely be approached by the agencies directed by the Trump EO to produce required reports, given the public-private partnerships already established in this area. The reviews required by the new EO cannot be undertaken by the federal government acting alone, as acknowledged for example in the EO's direction to the Secretary of Energy to consult not only with state, local and tribal governments but also "with others as appropriate."[14] The new EO furthermore provides a prompt for parties affirmatively to make their interests and concerns known to those agencies tasked to undertake the required analyses. What is more, private parties may seek to make their interests and concerns known to the White House itself, either directly in the near term or through their contributions to the reviews and assessments the new EO requires.

In addition, the new EO seems likely to reinvigorate the efforts of coordinating bodies like the ESCC, given not only the ESCC's now-recognized role in promoting the security of critical energy infrastructure

but also the new EO's charge to the Secretary of Energy to assess "the potential scope and duration of a prolonged power outage associated with a significant cyber incident."[15] That project picks up where the previous Administration left off, which is to say with public-private energy sector coordination through organizations such as the ESCC, CRISP and E-ISAC. Conclusions about the scope and duration of potential power outages will inevitably require understanding of industry's informational networks, protocols, and emergency capacities, learned among other ways through the emergency exercises that organizations like the ESCC have run.

The new EO may also provide an opportunity for electricity subsector stakeholders to advocate for the issuance of the final DOE rule governing how the Secretary of Energy's new emergency authorities would be exercised. Although the FAST Act required DOE to issue the rule within 180 days of its passage,[16] the rule has not been finalized (possibly in part due to the Trump Administration's EO requiring executive agencies to rescind two rules for each new rule they issue). But topics like how emergency orders issued in response to a grid security emergency may be communicated and enforced are centrally relevant to the review the new EO has tasked to the Secretary of Energy. Indeed, some stakeholders may press the point further — arguing that the rule not finalized may present an obstacle to maximum coordination between the government and private parties, and inhibit the quick execution of any emergency order the Secretary of Energy might issue in response to a grid emergency.

Finally, the new EO provides occasion for private parties to consider their own policies and protocols as well, and in particular, how those might be enhanced through government cooperation. For example, as noted, the new EO directs the Secretary of Homeland Security and other federal leaders to "engage section 9 entities," — *i.e.*, entities identified under Section 9 of EO 13636 as "owning or operating infrastructure for which a cybersecurity event could have catastrophic regional or national effects" — and to "solicit [their] input" in evaluating whether existing authorities and capabilities can best be employed to manage cyber risks.[17] For one concrete example of how entities like power generators, transmission companies, and grid operators might evaluate the extent to which existing authorities and capabilities facilitate their management of cyber risks, such entities might consider whether they and their personnel have sufficient security clearances to address cyber risks. Under EO 13636, the Secretary of Homeland Security is to expedite security clearances for appropriate personnel employed by critical infrastructure owners and operators.[18] For another example, private companies might assess their own cybersecurity and resilience by considering the extent to which existing cybersecurity capabilities at national laboratories can be most usefully employed to assist industry.

Conclusion

The federal government will necessarily lead efforts to protect the nation's critical infrastructure. Its informational resources, not to mention its ability to engage in offensive cyber activities, distinguish the government from private entities in important ways. The premise of the new cyber EO, like those of the previous Administration, is that the government and owners of critical infrastructure must work not merely in parallel, but rather in collaboration, to best manage cyber risks. By directing reviews of existing cybersecurity safeguards, and by requiring senior executive branch officials to engage with owners and operators of critical infrastructure, including critical electric infrastructure, the Trump EO provides an opportunity for private parties to reengage with the federal government to reduce cybersecurity risks.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Steven P. Croley*
steven.croley@lw.com
+1.202.637.3328
Washington, D.C.

Serrin A. Turner
serrin.turner@lw.com
+1.212.906.1330
New York

Admitted to practice in Michigan. D.C. and Illinois bar applications pending. D.C. Rule 49 notice: while bar application is pending, all legal services rendered under the guidance of an active D.C. bar member.

You Might Also Be Interested In

Ransomware Attacks: When Is Notification Required?

NYSDFS Revises Cybersecurity Rules to Accommodate Industry Concerns

Behind the Headlines of Evolving Cyberthreats (video)

Global Privacy & Security Compliance Law Blog

Endnotes

[1] Executive Order 13636 §7.

[2] Presidential Policy Directive/PPD – 21 (February 12, 2013) at 4, 11.

[3] Executive Order -----, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (May 11, 20017) §2(e)(1).

[4] See, e.g., Electricity Subsector Coordinating Council, http://www.electricitysubsector.org/.

[5] See, e.g., Energy Sector cybersecurity Preparedness, https://www.energy.gov/oe/energy-sector-cybersecurity-preparedness (describing CRISP program).

[6] See, e.g., Electricity ISAC, http://www.nerc.com/pa/ci/esisac/Pages/default.aspx.

[7] 16 U.S.C. §824o-1 (a)(7).

[8] *Id.* at (a)(7)(A)(i).

[9] *Id*. at (b)(1).

[10] *Id*. at (b)(3).

[11] *Id*. at (b)(6).

[12] *Id*. at (d)(1)-(2).

[13] *Id*. at (b)(1).

[14] Executive Order -----, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" §2(e).

[15] *Id*. at 2(e)(i).

[16] 16 U.S.C. §824o-1 (b)(1).

[17] Executive Order -----, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" §2(b)(i)-(ii).

[18] EO 13636 §4(d).