UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

ENSURING THE CONTINUED SECURITY OF THE UNITED STATES CRITICAL ELECTRIC INFRASTRUCTURE	**)** **)** **)** **)**	**86 Fed. Reg. 21309-01**

LIMITED COMMENTS OF SECURITYSCORECARD TO REQUEST FOR INFORMATION ON ENSURING THE CONTINUED SECURITY OF THE UNITED STATES CRITICAL ELECTRIC INFRASTRUCTURE

SecurityScorecard, Inc. offers limited comments to the United States Department of Energy (the "Department" or "DOE") Notice of Request for Information (the "RFI") issued in the above-captioned proceeding on April 22, 2021. The DOE seeks "information from electric utilities, academia, research laboratories, government agencies, and other stakeholders" in "appropriately balanc[ing] national security, economic, and administrability considerations" to enhance the security of American critical electric infrastructure. RFI, Introduction, Section A. As a private sector partner offering best-in-class cybersecurity ratings across industries, including critical infrastructure, SecurityScorecard is uniquely positioned to respond to RFI Subsection II.A.3, querying what actions the Department takes to facilitate responsible and effective procurement practices in the private sector.

I. INTRODUCTION AND BACKGROUND ON SECURITYSCORECARD

SecurityScorecard encourages the DOE to underscore the importance of monitoring third party risk as part of its education outreach to Bulk Electric System Cyber Systems procurers. While cyber diligence may form part of standard procurement processes, most procurers do not have the capacity or a standardized framework within which to meaningfully evaluate cyber risk on a continuous basis across their many vendors and service providers, thereby posing a risk to the security of the electric grid. With the administration's American Jobs Plan proposing to devote billions to infrastructure and grid modernization to the energy sector, the need for reliable and streamlined cyber diligence tailored to the energy sector is

broad and imminent.

SecurityScorecard is an industry-leading cybersecurity ratings platform that helps companies understand, improve, and communicate their own and their service providers' cybersecurity risk to management, directors, investors, employees, insurers, and increasingly, regulators. Backed by, amongst other investors, GV (Google Ventures), Riverwood Capital, Silver Lake Waterman, and Fitch Ventures, more than 20,000 users worldwide use its platform including top global pharmaceutical companies, major financial institutions, and at least 100 of the Fortune 500. SecurityScorecard data is also in use by supply chain risk management programs across various DoE, DHS, and DoD entities and State and local governments across the United States. SecurityScorecard's A-F ratings system, generated through publicly available data, measures an entity's cybersecurity hygiene across ten risk categories, including endpoint security (directional guidance on the state of client application updating/patching), network security (network service exposures to public internet as well as crypto issues), DNS health (which detects insecure configurations and vulnerabilities related to the domain name system), Patching Cadence (identifies out of date company assets that may contain vulnerabilities or risks), IP Reputation (measures amount of suspicious activity such as malware or spam emanating from the company's IP space), and Application Security (which measures common website application vulnerabilities). Its ratings provide a dynamic assessment that take into account evolving cybersecurity threats, with each organization's rating updated every 24 hours. Traditional cyber assessments offer only a static, point-in-time look at a company's cybersecurity posture. Leading cybersecurity ratings platforms like SecurityScorecard also monitor for new threats, such as zero-day computer software vulnerabilities, and incorporate those threats into their ratings dashboards to help alert entities to previously unknown exposures within themselves or across their supply chain. Cybersecurity ratings can aid Bulk Electric System Cyber Systems procurers in achieving economies of scale in the cyber diligence context by standardizing the diligence process and allowing procurers to monitor service providers more effectively and efficiently on a continuous basis. This defensive approach to cyber risk can yield tremendous downstream protection for companies, including entities operating or supporting American critical electric infrastructure.

II. SECURITYSCORECARD IDENTIFIES THREE AREAS OF OPPORTUNITY WITHIN THE AUTHORITY OF THE DEPARTMENT, FERC, AND NERC TO FACILITATE RESPONSIBLE AND EFFECTIVE PROCUREMENT PRACTICES FOR CRITICAL ELECTRIC INFRASTRUCTURE

A. Consider Voluntary Cybersecurity Ratings in Educational Industry Programming

In light of its working relationships with the North American Electric Reliability Corporation ("NERC"), the Federal Energy Regulatory Commission ("FERC"), DHS the Electricity Subsector Coordinating Council, trade forums, and the private sector, the Department is uniquely situated to educate industry on private sector opportunities to further responsible and effective procurement practices. SecurityScorecard recommends that the DOE consider the benefits of endorsing cybersecurity ratings in educational industry programming through its public-private partnerships, including with the Electricity Information Sharing and Analysis Center (E-ISAC), to facilitate industry's implementation of comprehensive risk management practices, specifically with respect to procurement. DOE endorsing cybersecurity ratings as a voluntary best practice throughout its public-private partnerships would accelerate information sharing, in that those subscribing to a cyber ratings service would acquire new security information and notify E-ISAC or peer companies of threats they have identified to their own supply chains. Additionally, the E-ISAC could subscribe to a security ratings service itself to monitor security trends or commonly used vendors for the sector, enhancing its own ability to respond to cyber vulnerabilities and threats. In that vein, it is important that the Department's endorsement underscore the value-add of continuous, dynamic ratings as opposed to static cybersecurity assessments, which may not accurately reflect the current cyber posture of an organization. SecurityScorecard also recommends that the Department endorse ratings systems that are fair and offer transparent scoring methodologies, for example, by making public rates of misattribution and allowing entities to refute scores at no additional expense. The powerful benefits that entities stand to derive from cybersecurity ratings depend on the integrity of the ratings themselves.

The increasing importance of cybersecurity has prompted various stakeholders to publicly endorse ratings as a tool to mitigate vulnerabilities to the nation's cybersecurity infrastructure, including in the following contexts:

i. The Cybersecurity and Infrastructure Security Agency (CISA) National Risk Management Center recently launched a new cyber venture called System Cyber Risk Reduction, explicitly highlighting the utility of security ratings as a valuable metric of cyber risk.[1] A blog authored by CISA's Assistant Director for the National Risk Management Center states: "The emergence of security ratings has driven cyber risk quantification as a way to calculate and measure cyber risk exposure. These security ratings provide a starting point for companies' cybersecurity capabilities and help elevate cyber risk to board decision making. Entities can also use security ratings alongside strategic risk metrics to align cyber scenarios with material business exposure; rollup cyber risks with financial exposure to inform risk management decisions; and measure improvement of cyber risk reduction over time. This kind of work needs to happen in the boardroom and also amongst national security leaders."[2] CISA's endorsement of cybersecurity ratings calls important attention to how ratings have emerged as an industry-standard best practice.

ii. On May 12, 2021, U.S. President Joseph Biden issued his *Executive Order on Improving the Nation's Cybersecurity*. Section 4 of the order addresses the Federal Government's efforts to enhance software supply chain security, including by requiring that the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), in coordination with the Chair of the Federal Trade Commission, to "identify secure software development practices or criteria for a consumer software labeling program […] [to] "identify, modify, or develop a recommended label, or, if

[1] B. Kolasky, *A Risk-Based Approach to National Cybersecurity*, CISA blog (January 14, 2021), available online at: https://www.cisa.gov/blog/2021/01/14/risk-based-approach-national-cybersecurity.
[2] *Id.*

practicable, a tiered software security rating system [that] shall focus on ease of use for consumers and […] maximize[ing] participation."[3] Again, the order is compelling legitimization of security ratings as a key to enhancing supply chain security.[4]

iii. Last year, the Cybersecurity Solarium Commission recommended that Congress establish and fund a National Cybersecurity Certification and Labeling Authority, similar to Energy Star appliance ratings.[5]

iv. In 2017, the U.S. Chamber of Commerce described the potential of "reliable security ratings that are fair, accurate, and clear [to] enhance security across the economy."[6] In conjunction with security ratings companies, the Chamber also developed a concrete set of principles on which to generate cybersecurity scores.[7]

SecurityScorecard recommends that the DOE consider introducing cybersecurity ratings into its existing educational programming as a best practice for Bulk Electric System Cyber Systems procurers to monitor their own cybersecurity hygiene and vet that of vendors in their supply chains. High-scoring procurers could choose to highlight their score to gain added reputational benefits or to prove and maintain compliance with cybersecurity standards such as the NIST Cybersecurity Framework. Subscribing to a cybersecurity ratings service that offers continuous monitoring will also help entities identify their and their vendors' vulnerabilities and specific ways to harden their systems. Cybersecurity ratings provide procurers a powerful and cost-effective tool to diligence vendors' cybersecurity track records and identify security-focused suppliers of software and hardware and other materials used in the electric infrastructure supply chain.

---

[3] The White House, *Executive Order on Improving the Nation's Cybersecurity*, May 12, 2021, available online at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[4] *Id.*

[5] United States of America Cyberspace Solarium Commission, *March 2020 Final Report*, available at: https://perma.cc/8KC8-XHN4.

[6] A. Beauchesne, *Why We Need Fair and Accurate Cybersecurity Ratings,* U.S. Chamber of Commerce (June 20, 2017, 9:00 AM), available online at: https://www.uschamber.com/series/above-the-fold/why-we-need-fair-and-accurate-cybersecurity-ratings.

[7] U.S. Chamber of Commerce, *Principles for Fair and Accurate Security Ratings*, (June 20, 2017, 10:00 AM), available online at: https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings.

Cybersecurity ratings have emerged as an industry-standard measurement and reliable way to ensure that regulated entities are taking a holistic approach to protecting their own and third party infrastructure. Their widespread adoption (over 5 million organizations scored daily and 20,000 users of just SecurityScorecard's ratings) may be facilitated by procurers' established business relationships: for example, certain ratings platforms offer their services through managed security service providers (MSSPs) or global systems integrators, relationships that many procurers already have in place. The DOE should have full expectation that cybersecurity ratings will come to be perceived and employed by utilities to signal their commitment to security, and the Department should play an active role in their uptake.

B. Offer Economic Incentives for Electric Utilities to Voluntarily Adopt Cyber Ratings

SecurityScorecard recommends that the DOE work with FERC, the exclusive economic regulator of the Bulk Electric System, to offer economic incentives for an electric utility's voluntary expenditures on cybersecurity ratings. The DOE could champion, for example, the use of federal programs such as tax credits to incentivize voluntary cybersecurity ratings expenditures, and should consider doing so over the long-term. The DOE and FERC could accelerate the adoption of responsible procurement by leveraging FERC's authority over financial mechanisms. For example, relatively quickly and consistent with the Administrative Procedures Act, FERC could issue a policy statement or rulemaking authorizing economic incentives for an electric utility's voluntary cybersecurity-related expenditures based on sections 205[8], 206[9], and/or 219[10] of the Federal Power Act. As natural monopolies, transmission companies regulated by FERC are compensated based on a specified return over their cost to provide services (cost-of-service rates). To incentivize transmission companies to voluntarily meet FERC's policy objectives, FERC often adopts economic incentives through rulemakings to encourage certain behaviors or investments. For example, FERC recently proposed adding Section 35.48(c)(2) to the FERC regulations to allow a public utility to

[8] 16 U.S.C. § 824d.
[9] 16 U.S.C. § 824e.
[10] 16 U.S.C. § 824s.

seek incentive-based financial treatment for certain classes of cybersecurity-related expenses, including "implementation expenses, such as system assessments by third parties or internal system reviews and initial responses to findings of such assessments."[11] FERC's proposal permits public utilities that make voluntary eligible cybersecurity capital investments to request a 200-basis point return on equity adder, which offers a significant incentive to voluntarily harden their cybersecurity systems.[12] SecurityScorecard recommends a policy statement in the short term, and a Rule in the long-term, explicitly qualifying voluntary cybersecurity ratings expenditures as eligible for incentive-based financial treatments as a procurement best practice.

Market-based technologies operating in the electric infrastructure sector (such as independent power producers that typically rely on market-based agreements and revenues) should also be able to secure compensation outside of market revenues for voluntary cybersecurity expenditures. Specifically, SecurityScorecard recommends that FERC allow for separate recovery of expenditures made in connection with the implementation of cybersecurity ratings. Market participants could recover their expenditures as part of a separate reliability-based service on top of market revenues for hardening their systems as reliable assets to the electric grid.[13]

Economic incentives for an electric utility's voluntary expenditures on cybersecurity ratings would help procurement practices evolve, enhance utilities' cybersecurity posture over the long-term, and create cost savings which would necessarily be passed on to consumers. Unlike command-and-control regulation, where regulated entities need only meet certain minimum thresholds to remain in compliance, financial incentives for cybersecurity ratings would induce industry to continuously optimize their cybersecurity practices, and at a much faster pace since private-sector participants respond quickly to increased operating margins.

---

11 *Cybersecurity Incentives,* Notice of Proposed Rulemaking, 173 FERC ¶ 61,240 at 41 (2020).

12 *Id*. at 32.

13 *See e.g. ISO New England Inc.*, 171 FERC ¶ 61,160 (2020) (accepting a cost-based mechanism for ISO New England market participants to recover critical infrastructure protection costs incurred to come under compliance with the requirements for facilities that ISO-NE identifies as critical to the derivation of Interconnection Reliability Operating Limits).

C. Incorporate Cyber Ratings into Reliability Standard Framework

The increased scrutiny on cybersecurity hygiene, particularly in the wake of the recent high-profile attacks targeting American critical infrastructure, such as the ransomware attack on Colonial Pipeline, should prompt FERC and NERC to consider incorporating cybersecurity ratings into the Reliability Standards Framework using their jurisdiction under the Federal Power Act.[14] FERC and NERC should utilize cybersecurity ratings as a security metric for registered entities' overall cyberhealth: for example, SecurityScorecard correlates low cybersecurity scores with increased likelihood to a cyberattack. Additionally, the SecurityScorecard platform can easily be configured to provide continuous compliance of the elements of the NERC's Critical Infrastructure Protection ("CIP") framework that can be observed outside of a company's firewall.

Requiring applicable NERC-registered entities to diversify the ways in which they manage risk will enhance the security and resilience of the electric grid. SecurityScorecard recommends that FERC and NERC incorporate cybersecurity ratings into NERC-CIP supply chain Reliability Standards. Cybersecurity ratings could be incorporated, for example, in CIP-013, which mandates mitigating cybersecurity risks to the bulk power system through the implementation of security controls for supply chain risk management.[15] The current version of the Reliability Standard requires applicable entities to consider and address security risks posed by vendor products and services.[16] A future version of CIP-013 could, for example, require or incentivize the use of cybersecurity ratings for certain high-risk procurements, or mandate the adoption of cybersecurity ratings as an element of supply chain risk management plans.

Finally, FERC and NERC should consider offering a cybersecurity ratings "safe harbor" in connection with supply chain cybersecurity incidents. For example, FERC and NERC could pledge that NERC-registered entities that made a procurement decision in reliance on a vendor's qualifying score as

---

[14] 16 U.S.C. § 824o(b)(1).

[15] NERC, Reliability Standard CIP-013-2 (Cyber Security - Supply Chain Risk Management), https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-013-2&title=Cyber%20Security%20-%20Supply%20Chain%20Risk%20Management&Jurisdiction=United%20States.

[16] *Id.*

issued by a Department-authorized cybersecurity ratings platform will not be the subject of a related enforcement action. Whereas a command-and-control approach would lead NERC-registered entities to improve their cybersecurity posture only up to a certain minimum threshold barring additional incentives, SecurityScorecard's recommendation places the onus of managing cyber risk on registered entities. In turn, registered entities are incentivized to ensure that their (1) CIP compliance programs rely on only authorized cybersecurity ratings and (2) vendors continuously meet minimum scores to qualify for the safe harbor.

Incorporating cybersecurity ratings into NERC's CIP supply chain Reliability Standards would enhance applicable registered entities' cybersecurity hygiene and reward those that retain services from vendors with recognized and demonstrated security practices. Ultimately, incentivizing high-quality cybersecurity ratings encourages better risk-management practices and strengthens the resilience and reliability of the electric grid.

III. CONCLUSION

SecurityScorecard respectfully requests that the DOE consider the forgoing comments in this proceeding.

Respectfully submitted,

Sachin Bansal
General Counsel

June 7, 2021