March 13, 2020

The Cyberspace Solarium Commission's Final Report and Recommendations Could Have Implications for Business

On March 11, 2020, the Cyberspace Solarium Commission (the "CSC" or the "Commission")[1] published its Final Report,[2] which is the culmination of nearly a year of work, including approximately 30 meetings and 300 interviews.[3] The Report outlines more than 75 recommendations for how the federal government should act to defend against and deter cyberattacks on the federal government, state governments, the private sector, and private citizens.

The CSC is a bicameral and bipartisan commission that was established by the 2019 Defense Authorization Act. Charged with developing a comprehensive and strategic approach to defending the United States in cyberspace, the Commission is co-chaired by Sen. Angus King (I-Maine) and Rep. Mike Gallagher (R-Wisconsin) and has 14 commissioners, including four U.S. legislators, four senior executive agency leaders, and six nationally recognized experts from outside of government.[4]

A number of the more than 75 recommendations, if enacted, have practical implications for the private sector:

- **Establish "Final Goods Assembler" Liability (Recommendation 4.2)**. The recommended legislation would hold final goods assemblers ("FGAs") of software, hardware, and firmware liable for damages from incidents that exploit vulnerabilities that were known at the time of shipment or discovered and not fixed within a reasonable amount of time. An FGA is any entity that enters into an end user license agreement with the user of the product or service and is most responsible for the placement of a product or service into the stream of commerce. The legislation would direct the Federal Trade Commission ("FTC") to promulgate regulations subjecting FGAs to transparency requirements, such as disclosing known, unpatched vulnerabilities in a good or service at the time of sale.

---

1 The term "Solarium" is a reference to Project Solarium, a commission created by President Eisenhower to establish measures to respond to Soviet expansionism during the Cold War. The commission met in the White House's solarium room.

2 The full report is available here: https://www.solarium.gov/report.

3 Tim Starks, *Panel outlines massive federal cybersecurity overhaul*, Politico (Mar. 11, 2020), https://www.politico.com/news/2020/03/11/panel-outlines-massive-federal-cybersecurity-overhaul-125287?nname=playbook-pm&nid=0000015a-dd3e-d536-a37b-dd7fd8af0000&nrid=00000151-e36b-ded2-ad77-ef6b67fe0001&nlid=964328.

4 Robert Chesney, *The Cyberspace Solarium Commission Report: A Lawfare Series*, Lawfare Blog (Mar. 11, 2020), https://www.lawfareblog.com/cyberspace-solarium-commission-report-lawfare-series.

- **Establish a Bureau of Cyber Statistics (Recommendation 4.3)**. The Bureau of Cyber Statistics would be charged with collecting and providing statistical data on cybersecurity and the cyber ecosystem to inform policymaking and government programs. Companies that regularly collect cyber incident data as part of their business would be required to provide aggregated, anonymized, minimized data on cyber incidents to the Bureau of Cyber Statistics on an annual basis. Private companies that provide data to the Bureau of Cyber Statistics would be insulated from liability associated with the disclosure of such data.

- **Amend the Sarbanes-Oxley Act to Include Cybersecurity Reporting Requirements (Recommendation 4.4.4)**. Among other things, the amendment would (1) specify corporate responsibility requirements for the security of information systems; (2) mandate that public companies maintain internal records of cyber risk assessments; and (3) require management assessments and attestation of plans to manage risk from information systems and data.

- **Pass a National Data Security and Privacy Protection Law (Recommendation 4.7)**. The National Data Security and Privacy Protection Law would establish national minimum common standards for the collection, retention, analysis, and third-party sharing of personal data; thresholds to determine which entities are covered by the legislation; and timelines for deleting, correcting, or porting personal data upon request. It would also explicitly establish a duty of care for covered entities, requiring such entities to exert reasonable care and security regarding the protection of all relevant data they hold. The FTC would be charged with enforcing these standards with civil penalties.

- **Pass a National Breach Notification Law (Recommendation 4.7.1).** As recommended, the National Breach Notification Law would establish a threshold for what could constitute a breach covered by the law; notification requirements, including standards and timelines for notifying victims; transmission of relevant forensic data to appropriate authorities; and preempt the 54 existing state, district, and territorial data breach notification laws already in place.

- **Clarify Liability for Federally Directed Mitigation, Response and Recovery Efforts (Recommendation 3.3.2)**. This recommendation calls on Congress to pass laws that would insulate the private sector from liability for taking actions at the direction of federal government agencies "to protect against or respond to an emergency or threat relating to a cybersecurity incident impacting national security."

- **Empower Departments and Agencies to Serve Administrative Subpoenas in Support of Threat and Asset Response Activities (Recommendation 5.1.3)**. This recommendation calls on Congress to pass laws that would grant government agencies administrative subpoena powers in furtherance of the government's efforts to identify and respond to cyber threats, vulnerabilities, and attacks on critical private sector infrastructure. The recommendation specifically contemplates

extending this administrative subpoena power to the FBI and Secret Service for violations of the Computer Fraud and Abuse Act.

Implications

The Commission's Report is wide-reaching and ambitious. Although the Report is action-oriented and urgent in its tone, it may take years before any of the Commission's recommendations are substantively implemented by Congress or the White House. If the Report does gain traction, a wide range of industries and businesses would be impacted by legislation or executive actions implementing the CSC's recommendations. We will continue monitoring for developments and report any further activities.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Robert A. Atkins
+1-212-373-3183
ratkins@paulweiss.com

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Jonathan S. Kanter
+1-202-223-7317
jkanter@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Richard C. Tarlowe
+1-212-373-3035
rtarlowe@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Associates Daniel J. Klein and Apeksha S. Vora contributed to this Client Alert.