GIBSON DUNN

April 18, 2023

THE BIDEN ADMINISTRATION SIGNALS NEW DIRECTION FOR CYBERSECURITY

To Our Clients and Friends:

The Biden administration has been steadily evolving its views of national security risks and priorities—and what measures the executive branch will take to mitigate those risks. Last fall's National Security Strategy called out critical technology and cybersecurity as key national security concerns. This focus sharpened with the release of the National Cybersecurity Strategy last month. And, most recently, the administration has submitted a $3.1 billion budget request for the Cybersecurity and Infrastructure Security Agency (CISA), a 22 percent increase from its request last year, to implement that strategy and fund other initiatives. While strategy is not policy, and budget proposals are not appropriations, these are strong signals of the shifting winds of the administration regarding the tools and incentives the administration will deploy to mitigate cybersecurity risks.

After years of relying on largely voluntary standards to encourage companies to harden their cybersecurity defenses, interspersed with incentives including funding and grants, the administration has definitively taken the position that it does not think companies have done enough. Accordingly, the new cybersecurity strategy calls for a heavier hand. Should the strategy be implemented, companies can expect to see direct liability, new regulations, and lawsuits from the federal government itself for companies that fail to make secure products, do not adopt minimum security measures, or misrepresent the actions they have taken. These new measures come as the administration is increasingly focused on strategic competition with China.

Below, we highlight the four main tools that companies should know about that the Biden Administration has vowed to use to secure critical infrastructure and industry from cyber threats.

1. **Direct liability for software vendors**. First, the Biden administration says that software companies and vendors should be directly liable for failing to adopt "reasonable" security measures into the programs used to power critical infrastructure and other areas. The administration said it has been unhappy with voluntary efforts to increase software security, which have made progress but has been inconsistent across industries. And, because the administration believes that software vendors and companies that control data are in the best position to address this liability, it said that they should bear responsibility for failing to adopt those reasonable measures and not their end users and infrastructure providers who will be impacted by those failures directly."

   We're all walking around with unsafe technology. So we have to change the incentives," CISA Director Jen Easterly told a House subcommittee recently as she sought funding for the federal

government's efforts. "We may need to look at certain liability for whether manufacturers have duty of care to be able to protect those consumers."

The legislation the administration is contemplating to implement this liability would prohibit software terms of service from disclaiming all liability for security flaws, even if the flaw is from open-source software that has been integrated into the commercial project, and would also impose higher standards of care in high-risk areas.

2. **New rulemaking and legislation to fill in regulatory gaps**. Second, in addition to legislation on direct liability, the administration is planning new rulemaking and other legislation to close gaps in existing law that impose minimum security standards in a host of industries. In particular, cloud-based services are not all covered by existing regulations despite being integrated into systems across industries. These new regulations should be "performance-based," the administration said, and modeled after voluntary frameworks from the National Institute of Standards and Technology (NIST) and CISA.

   This comes in the wake of other rulemaking for such standards in the oil and gas pipeline, aviation, rail, and water sectors. And other legislative efforts have also advanced security measures, such as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) that requires critical infrastructure providers to notify federal authorities about cybersecurity incidents. The administration is advancing rulemaking to implement CIRCIA as well, with CISA in the lead.

   The administration seeks to pair these new requirements with new funding and financial incentives to speed compliance. While some companies can absorb these costs, others have low margins that make this difficult. Thus, in those areas, the administration is encouraging regulators to tilt incentives to reduce these costs, such as through favorable tax and rate-setting arrangements. Such arrangements would be on top of the funding that the government is already pouring into this area through the CHIPS and Science Act, the Inflation Reduction Act, and the Bipartisan Infrastructure Law. Further, the administration said it is exploring a government-backed support for the cyber insurance market to protect it in the event of a catastrophic event.

3. **Government to lead the way—including as a plaintiff**. Third, in all of these areas, the administration also signaled that it will itself set the bar for private industry to follow, such as by updating its own technology and through procurement processes to test new cybersecurity requirements, and will update its own technology using standards that it wants private industry to adopt as well. For example, the administration is prioritizing cryptography upgrades to public computer networks to be resistant to quantum-based efforts to compromise those networks. This is not just to secure the government's own networks but also to set the bar that it expects the private sector to follow.

   The administration has also signaled it will increase regulatory harmonization, make it easier for companies reporting an incident to connect with the appropriate officials quickly, modernize federal technology, and engage in research and development efforts. Given the increasing

patchwork of notification requirements and various government equities in cyber incidents, such harmonization is critical to reducing the regulatory burden on companies—particularly during the high operational tempo of cyber incident response.

The federal government has indicated that it will continue to bring actions to enforce cybersecurity commitments. For example, the Department of Justice has already used the False Claims Act to pursue companies that allegedly misrepresent cybersecurity commitments in their federal contracts. And the Department of Justice has also launched a new nationwide "disruptive technology strike force" with the Commerce Department to coordinate efforts to respond to threats to critical infrastructure.

4. **Shifting focus from criminal groups to state actors**. Finally, the administration has signaled that the central threat that it has built its strategy around is from state actors. While criminal groups using ransomware to extract groups are still addressed by the administration's strategy, it is the governments of China, Russia, Iran, and North Korea where the strategy is focused. The administration has highlighted the efforts of those state actors, and in particular China, to carry out cyber attacks and compromise vulnerable infrastructure. In an echo of the National Security Strategy, the cybersecurity strategy highlights that China "now presents the broadest, most active, and most persistent threat." And also without naming China, the strategy notes that domestic networks should reduce their dependence "on critical foreign products and services from untrusted suppliers," pointing to the longstanding controversy over China-based companies that supply hardware and equipment for U.S. computer networks.

   The administration's cybersecurity strategy further highlights the administration's increased cross-border efforts to coordinate cybersecurity efforts with Australia, the United Kingdom and other European countries, India, Japan, and others.

In sum, the key takeaways for private industry in the administration's cybersecurity strategy, as reinforced by budget priorities, are that companies in an ever-wider set of industries will not only be tempted into compliance with new funding or cajoled from the bully pulpit to increase their cybersecurity measures, but will also have to contend with a more forceful response from government that will expect them to meet security standards and promises—and face liability if they fail to do so. This increased enforcement may also be complicated by multiple agencies pursuing the same actions, resulting in the potential for companies having to deal with overlapping and uncoordinated inquiries. And with the increasing focus on state actors in place of cybercriminals, the strategy shows less of a focus on private ransomware issues and an increasing national security response that may serve as a prioritization filter. While the strategic objectives outlined in the cyber strategy and backed by the budget proposal will require significant executive action prior to coming into effect, companies should prepare now to meet the shifting approach towards increased cybersecurity requirements and liability.

The following Gibson Dunn lawyers assisted in preparing this alert: Alexander Southwell, Stephenie Gosnell Handler, and Eric Hornbeck.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity & Data Innovation practice group:

United States

S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)
Jane C. Horvath – Co-Chair, PCDI Practice, Washington, D.C. (+1 202-955-8505, jhorvath@gibsondunn.com)
Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com)
Gustav W. Eyler – Washington, D.C. (+1 202-955-8610, geyler@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)
Svetlana S. Gans – Washington, D.C. (+1 202-955-8657, sgans@gibsondunn.com)
Lauren R. Goldman – New York (+1 212-351-2375, lgoldman@gibsondunn.com)
Stephenie Gosnell Handler – Washington, D.C. (+1 202-955-8510, shandler@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
Vivek Mohan – Palo Alto (+1 650-849-5345, vmohan@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Rosemarie T. Ring – San Francisco (+1 415-393-8247, rring@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)

Europe

Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Joel Harrison – London (+44(0) 20 7071 4289, jharrison@gibsondunn.com)
Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com)

Asia

Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)