Skadden

Privacy & Cybersecurity Update

Biden Administration Announces Proposed Voluntary Cybersecurity Labeling Program for Smart Devices

On July 18, 2023, President Joe Biden's administration announced a proposed cybersecurity certification and labeling program to help American consumers choose smart devices that have stronger cybersecurity protections and that are less vulnerable to cyberattacks. The program is one part of the administration's National Cyber Strategy, which was released earlier this year.

Background

The Biden administration's announcement of the proposed U.S. Cyber Trust Mark Program is an effort to raise the bar for cybersecurity across common devices, including various internet-of-things (IoT), connected or "smart" devices such as refrigerators, microwaves, televisions, climate control systems and fitness trackers. IoT devices have been considered to have weak cybersecurity as many devices ship with simple default passwords and do not offer regular security updates. The program, which has been adopted in similar form in Singapore and other countries, was based on a recommendation made by the U.S. Cyberspace Solarium Commission in its March 2020 report.[1] In its announcement, the Biden administration confirmed that the Federal Communications Commission (FCC) will lead the program under its authority to regulate wireless communications devices and would begin regulating the labeling of smart devices based off cybersecurity standards published by the National Institute of Standards and Technology (NIST).[2]

Should the program be adopted by the FCC after a vote by its commissioners and a public comment period, companies that manufacture or distribute common devices, such as IoT, connected or "smart" devices, should consider whether to opt-in to help assure the public that they are purchasing and using safe and secure products.

[1] See U.S. Cyberspace Solarium Commission's March 2020 report "Senator Angus King & Representative Mike Gallagher, Official Report." Key recommendation 4.1 of the report contemplates establishing a National Cybersecurity Certification and Labeling Authority, which would establish and manage a program for voluntary security certifications and labeling of information and communications technology products.

[2] See July 18, 2023, White House release "Biden administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers."

© Skadden, Arps, Slate, Meagher & Flom LLP. All rights reserved.

US Cyber Trust Mark Logo

The program, which would be voluntary and is expected to be up and running in 2024 if approved, seeks to help American consumers make informed decisions about the relative security of the "smart" products they choose to purchase and use.

In particular, the newly created "U.S. Cyber Trust Mark" would be applied to products meeting established cybersecurity criteria in the form of a distinct shield logo. The logo has not yet been finalized and the FCC is currently applying to register a logo with the U.S. Patent and Trademark Office.[3] The Biden administration, including the Cybersecurity and Infrastructure Security Agency (CISA), has indicated it would support the FCC encouraging major U.S. retailers to prioritize and highlight products that utilize the logo when offering smart devices for sale.

Trust Mark Cybersecurity Standards

As currently proposed, the program would leverage stakeholder-led efforts to certify and label products based on the cybersecurity standards as published by NIST. Currently, the standards include, for example, requiring unique and strong passwords, data protection, software updates and incident detection capabilities. Several leading manufacturers and retailers have indicated their support and commitment to advance the program.

NIST will begin working on standard cybersecurity requirements for consumer-grade routers, which, if compromised, may be used to eavesdrop, steal passwords and attack other devices and high-value networks. NIST seeks to complete such efforts by the end of 2023 to permit the FCC to consider expanding the program to cover consumer-grade routers. In addition, the U.S. Department of Energy National Laboratories will collaborate with industry partners to develop cybersecurity labeling requirements for smart meters and power inverters, which are essential to the future development of clean, smart power grids.

Next Steps

The FCC intends to use a QR code on the label of each smart product that would link to a national registry of certified devices and provide consumers with relevant security information for each product. The U.S. Department of State also intends to support the program by engaging allies and other partners in hopes of harmonizing standards and securing mutual recognition of similar labeling programs. Furthermore, in alignment with the Biden administration's National Cyber Strategy, the federal government may choose to prioritize vendors with labeled products in its procurement practices.[4]

Key Takeaways

Companies that manufacture or distribute smart devices should continue to monitor the FCC for guidance on the program, as well as NIST or other standard-setting organizations for updates to cybersecurity labeling standards. Such companies also should consider evaluating their cybersecurity practices as they pertain to the NIST Cybersecurity Framework to identify any potential gaps between company practices and the current NIST standards.

Return to Table of Contents

NIST Releases Draft Version of Its Cybersecurity Framework 2.0

NIST has released a new version of its widely used cybersecurity framework following a public comment period, marking the first major overhaul to the framework in almost a decade.[5]

On August 8, 2023, after considering almost a year's worth of public commentary, NIST issued an extensive update to its cybersecurity framework (CSF), a voluntary set of guidelines that organizations have relied on to better understand, reduce and communicate about cybersecurity risk since its initial publication in 2014. With the release of the draft framework, referred to as the Cybersecurity Framework 2.0 or CSF 2.0, NIST seeks to increase applicability across a wider range of industries, address changes in the cybersecurity landscape, improve guidance on implementation of the CSF (including in conjunction with other resources from NIST and elsewhere) and emphasize cybersecurity governance.

Notable Changes in Draft Version of CSF 2.0

The CSF 2.0 places greater emphasis on overall governance by creating a sixth pillar, the "govern" function, in addition to the original five pillars of the CSF — identify, protect, detect, respond and recover. This new pillar addresses how organizations can make and execute their own internal decisions to support their overall cybersecurity strategy. The emphasis on governance is a recognition that cybersecurity is a major source of enterprise

[3] The proposed logos can be viewed on the FCC's website.

[4] See the White House's National Cyber Strategy here. Under strategic objective 3.5, the strategy notes the federal government may use its vendor contracts and procurement power to improve the accountability of vendors that sell to the federal government.

[5] The NIST Cybersecurity Framework 2.0 is available here.

risk that requires constant vigilance similar to that required with respect to businesses' legal and financial risks.

In addition, supply chain risks and the widespread threat of ransomware are recognized as cybersecurity threats that particularly are of concern. In response, the CSF 2.0 reflects NIST's latest guidance on cybersecurity supply chain risk management and secure software development, as well as updates made to other NIST resources in recent years, such as the NIST Privacy Framework 1.0 and the Artificial Intelligence Risk Management Framework 1.0.

As a pathway to address new technologies and evolving cybersecurity risks on a go-forward basis, and to provide further guidance to organizations with respect to implementation of the CSF, NIST will maintain notional examples of action-oriented processes to achieve conformity with CSF guidance, referred to as "Implementation Examples," on its CSF website. Draft versions of initial Implementation Examples have been released under separate cover for public comment.[6] NIST has requested feedback on what types of Implementation Examples would be most beneficial, how often the Implementation Examples should be updated, and whether and how to accept examples developed by the community.

The CSF 2.0 also significantly revises and expands its guidance on implementing "Framework Profiles," which enable organizations to establish a roadmap for reducing cybersecurity risk that is aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Framework Profiles can be used to describe the current state or the desired target state of an organization's cybersecurity outcomes.

Key Takeaways

NIST's release of the CSF 2.0 represents a material revision to the guiding standard for good cybersecurity practices that has been in place for almost a decade and reflects the current usage and usefulness of the CSF by and for a variety of different types of organizations. Companies managing critical infrastructure should therefore carefully review the updated version of the CSF. Relatedly, organizations of all sizes may find the CSF 2.0 to be a useful and valuable resource when developing or improving their cybersecurity compliance programs.

Return to Table of Contents

[6] The draft Implementation Examples are available here.

California Privacy Protection Agency and California Attorney General Appeal Delay of Enforcement of CPRA Regulations

The California Privacy Protection Agency (CPPA) and California Attorney General Rob Bonta filed a petition to overturn a recent trial court decision that delayed the enforcement of new regulations under the California Consumer Privacy Act of 2018 (CCPA) that implemented changes required by the California Privacy Rights Act (CPRA).

Background

As covered in our July 2023 *Privacy and Cybersecurity Update*, on June 30, 2023, a Sacramento County Superior Court judge agreed to delay the enforcement of certain portions of the CPRA regulations, stating that enforcement could only begin a year after the regulations were confirmed and delaying the compliance deadline for businesses subject to the CCPA. Pursuant to the decision, for 12 of the 15 issues addressed by the CPRA regulations, such regulations will take effect on March 29, 2024. The remaining three issues would have an enforcement date that is one year from the release of the finalized regulations addressing such issues.

Despite the Sacramento County Superior Court's decision, Mr. Bonta is continuing enforcement of the CCPA and regulations currently in force. On July 14th, 2023, the attorney general's office announced that it will be conducting an "investigative sweep" of large California employers' compliance with the CCPA's privacy protections of personal information of employees and job applicants, most of which came into force on January 1, 2023.

On August 4, 2023, the CPPA and Mr. Bonta released a statement announcing they filed a petition with California's Third District Court of Appeal to overturn the trial court's decision discussed above which imposed the deferred enforcement of the CPRA regulations. The CPPA emphasized the importance of Proposition 24's purpose, which was introduced as a ballot initiative to protect the privacy of California residents by expanding the state's consumer privacy laws. In the statement, CPPA General Counsel Philip Laird noted that "granting CalChamber's request to delay enforcement of portions of the regulations hurts not only consumers, but also those businesses that have operated in good faith to implement the protections required by the regulations."[7]

[7] See the CPPA and attorney general's statement here.

Key Takeaways

The CPPA anticipates that the Court of Appeal will decide whether to take the petition appealing the lower court's ruling in the next few weeks. In light of the attorney general's recent investigative sweeps, businesses should aim to finalize their compliance with the new CPRA regulations as soon as possible.

Return to Table of Contents

Colorado Attorney General Provides CPA Compliance Resources to Public

In August 2023, the Colorado attorney general added new resources to its public Colorado Privacy Act (CPA) website,[8] including FAQs with general information and descriptions of consumer rights, impacts on covered entities and planned enforcement, as well as examples of guidance letters sent to covered entities on July 10, 2023.

Background

The CPA, which went into effect on July 1, 2023, is a comprehensive data privacy law aimed at protecting the data and privacy of Colorado residents.[9] Colorado Attorney General Phil Weiser announced via a press release[10] on July 12, 2023, and a series of guidance letters sent to businesses the same week that the Colorado Department of Law would begin enforcing the CPA. The Colorado attorney general's office has now added to its public CPA website examples of these guidance letters as well as other resources (such as FAQs) aimed at educating the public and covered entities about the CPA. Covered entities that already comply with other comprehensive state privacy laws should nonetheless consider reviewing these resources since there are key differences between the CPA and the privacy laws of other states, outlined here:

- Unlike most U.S. state privacy laws, not-for-profit organizations are subject to the CPA.
- Companies that sell the personal data of Colorado residents or engage in targeted advertising must, by July 1, 2024, use the technologies enumerated on a list of approved universal opt-out mechanisms (to be published by the Colorado Department of Law no later than January 1, 2024).
- Unlike the California Consumer Privacy Act of 2018, which includes a regime for consumers to generally "opt-out" of the processing of sensitive personal information, the CPA requires controllers to obtain consent in advance to conduct any such processing.

Compliance With the CPA

The CPA grants Colorado consumers new rights with respect to their personal data, including rights to access, delete or correct their personal data and the right to opt out of its sale or use for targeted advertising or certain kinds of profiling.[11] The CPA also places new obligations on covered entities. For example, covered entities must give Colorado consumers meaningful information about the collection and use of their data, conduct data protection assessments and obtain consent before processing certain types of sensitive personal data. The attorney general's office has stated that its enforcement of the CPA is "a critical tool to protect consumers' data and privacy" and that if it becomes "aware of organizations flouting the law or refusing to comply with it," that it is "prepared to act."[12] Accordingly, covered entities (along with any entity seeking to determine if the CPA will apply to its activities), should consider taking advantage of the compliance resources provided on the CPA website, including:

- **Guidance Letters.** The initial round of guidance letters was focused on educating companies that operate in Colorado on their new legal obligations, with a particular emphasis on obligations relating to the collection and use of sensitive data, including the requirement to obtain consumer consent prior to collecting sensitive data, and the obligation to allow consumers to opt out of targeted advertising and profiling.[13] Thus, businesses that operate in Colorado and collect or use sensitive consumer data may especially benefit from reviewing the guidance letters now available.
- **FAQs.** The FAQs now available on the CPA website provide succinct guidance regarding the CPA, including the following highlights:
  - **Who must comply with the CPA?** The CPA applies to entities, including nonprofits, that conduct business in Colorado or deliver commercial products or services targeted to residents of Colorado; *and* either:
    - process the personal data of more than 100,000 individuals in any calendar year; or
    - derive revenue or receive discounts on goods or services in exchange for the sale of personal data of 25,000 or more individuals.

[8] See the Colorado Attorney General's Office's CPA website.

[9] See our June 2023 *Privacy & Cybersecurity Update* article "Colorado Comprehensive Privacy Law Goes Into Effect."

[10] See Colorado Attorney General Phil Weiser's press release dated July 12, 2023.

[11] The final rules for the CPA were filed on March 15, 2023. The rules include technical specifications for one or more universal opt-out mechanisms that clearly communicate a consumer's affirmative, freely given and unambiguous choice to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data (6-1-1313(2), C.R.S.).

[12] See the attorney general's press release.

[13] *Id.*

- The CPA also applies to service providers, contractors and vendors that manage, maintain or provide services relating to the data on behalf of these companies.
- The CPA does not cover the personal data of individuals acting in a commercial or employment context, such as a job applicant.
- **What does it mean to process data?** Data processing refers to actions a company may take regarding personal data, including the collection, usage, sale, storage, disclosure, analysis, deletion or modification of personal data. An entity is determined as processing data even if it instructs another entity to do so on its behalf.
- **What is the difference between personal data and sensitive data?** Personal data is any nonpublic information that reasonably can be linked to an individual. Sensitive data is a subset of personal data and includes:
  - any personal data regarding a child under the age of 13;
  - any data that reveals the race, ethnic origin or religious beliefs, mental or physical health conditions or diagnoses, sexual activity, preferences or orientation, or citizenship status or citizenship of an individual; and
  - biometric data that is used for identifying an individual.
- **Are companies provided notice of a violation before enforcement action is taken?** If the attorney general or district attorney determines that a violation can be remedied, they must first send a letter giving the violator 60 days to cure the violation. If either office determines that no fix is possible for the violation, no such letter is required. The process of providing notice of a violation and allowing 60 days for a cure will be in effect until January 1, 2025.

Key Takeaways

As enforcement of the CPA ramps up, covered entities — particularly those processing sensitive consumer data — should consider reviewing the compliance resources provided by the Colorado attorney general's office that are now available on the public CPA website.

Return to Table of Contents

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Avia M. Dunn
Partner / Washington, D.C.
202.371.7174
avia.dunn@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Maya P. Florence
Partner / Boston
617.573.4805
maya.florence@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Richard J. Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

David Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Nicole L. Grimm
Counsel / Washington, D.C.
202.371.7834
nicole.grimm@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

This communication is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This communication is considered advertising under applicable state laws.

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000