View on our website.

GIBSON DUNN

Securities Regulation & Corporate Governance Update

December 12, 2024

Cybersecurity Disclosure Overview: A Survey of Form 10-K Cybersecurity Disclosures by S&P 100 Companies

This update discusses key trends and insights from our analysis of the cybersecurity disclosures made by 97 S&P 100 companies in their most recent Form 10-K filings in response to Regulation S-K Item 106.

I. Introduction

This alert highlights key trends and insights from our analysis of the cybersecurity disclosures made by 97 S&P 100 companies in their 2024 Form 10-K filings, as required by new Item 106 of Regulation S-K ("Item 106"), as of November 30, 2024.[1]

As discussed in a previous client alert, the Securities and Exchange Commission ("SEC" or "Commission") adopted on July 26, 2023, a final rule requiring public companies to provide current disclosure of material cybersecurity incidents and annual disclosure regarding cybersecurity risk management, strategy, and governance. Under Item 106, which is required to be addressed in new Item 1C of Form 10-K, public companies must include disclosures in their annual reports regarding their (1) cybersecurity risk management and strategy, including with respect to their processes for identifying, assessing, and managing cybersecurity threats and whether risks from cybersecurity threats have materially affected them, and (2) cybersecurity governance, including with respect to oversight by their boards and management.[2] All public companies were required to comply with these disclosure requirements for the first time

beginning with their annual reports on Form 10-K or 20-F for the fiscal year ending on or after December 15, 2023.

II. Executive Overview

While certain disclosure trends have emerged under Item 106, we note that there is significant variation among companies' cybersecurity disclosures, reflecting the reality that effective cybersecurity programs must be tailored to each company's specific circumstances, such as its size and complexity of operations, the nature and scope of its activities, industry, regulatory requirements, the sensitivity of data maintained, and risk profile. Companies must strike a careful balance in their disclosures, providing sufficient decision-useful information for investors, while taking care not to reveal sensitive information that could be exploited by threat actors.[3] We expect company disclosures to continue to evolve as their practices change in response to the ever-evolving cybersecurity threat landscape and as common disclosure practices emerge among public companies.

Below is an executive overview of the key disclosure trends we observed (discussed in detail in Section III below):

- **Materiality.** The phrasing used by companies for this disclosure requirement varies widely. Specifically, in response to the requirement to describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect the company, the largest group of companies (40%) include disclosure in Item 1C largely tracking Item 106(b)(2) language (at times, subject to various qualifiers); 38% vary their disclosure from the Item 106(b)(2) requirement in how they address the forward-looking risks; and 22% of companies do not include disclosure specifically responsive to Item 106(b)(2) directly in Item 1C, although a substantial majority of these companies cross-reference to a discussion in Item 1A "Risk Factors."
- **Board Oversight.** Most companies delegate specific responsibility for cybersecurity risk oversight to a board committee and describe the process by which such committee is informed about such risks. Ultimately, however, the majority of surveyed companies report that the full board is responsible for enterprise-wide risk oversight, which includes cybersecurity.
- **Cybersecurity Program.** Companies commonly reference their program alignment with one or more external frameworks or standards, with the National Institute of Standards and Technology (NIST) Cybersecurity Framework being cited most often. Companies also frequently discuss specific administrative and technical components of their cybersecurity programs, as well as their high-level approach to responding to cybersecurity incidents.
- **Assessors, Consultants, Auditors or Other Third Parties.** As required by Item 106(b)(1)(ii), nearly all companies discuss retention of assessors, consultants, auditors or other third parties, as part of their processes for oversight, identification, and management of material risks from cybersecurity threats.
- **Risks Associated with Third-Party Service Providers and Vendors.** In line with the requirements of Item 106(b)(1)(iii), all companies outline processes for overseeing risks associated with third-party service providers and vendors.
- **Drafting Considerations.**

- Most companies organize their disclosure into two sections, generally tracking the organization of Item 106, with one section dedicated to cybersecurity risk management and strategy and another section focused on cybersecurity governance. Companies typically include disclosures responsive to the requirement to address material impacts of cybersecurity risks, threats, and incidents in the section on risk management and strategy.
- The average length of disclosure among surveyed companies is 980 words, with the shortest disclosure at 368 words and the longest disclosure at 2,023 words. The average disclosure runs about a page and a half.

While comment letters have not been issued in response to Item 106 disclosure in annual reports on Form 10-K filed by the S&P 100 companies we surveyed, as of November 30, 2024, five comment letters from the Staff had been issued to other companies regarding their Item 106 disclosures. For details, see Section VI below.

III. Key Disclosure Trends

For comparison purposes, we have grouped the discussion below into three categories: (1) cybersecurity risk management and strategy; (2) cybersecurity governance; and (3) disclosures in response to the requirement to address material cybersecurity risks, threats, and incidents.

a. Cybersecurity Risk Management and Strategy

Item 106(b)(1) calls for a description of a company's "processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes." In response to this overarching disclosure requirement, some of the most commonly addressed topics are as follows:

- **Cybersecurity Frameworks or Standards.** Though not specifically required by Item 106, a majority of surveyed companies (60%) reference one or more external frameworks or standards that inform, to varying degrees, their cybersecurity program management processes and practices. The NIST Cybersecurity Framework is referenced most often, with 51 companies making mention of it. Other frameworks or standards cited by surveyed companies include those set by the International Organization for Standardization (ISO) (including, for example, ISO 27001 and 27002), SOC 1 and 2, and the Payment Card Industry Data Security Standard (PCI DSS). Notably, companies use varied terminology when discussing specified frameworks or standards. For example, when citing NIST, companies explain that their cybersecurity program or risk management approach "leveraged," was "informed by," "aligns with," or was "based on" the framework.[4]
- **Description of Cybersecurity Program Elements.** Nearly all surveyed companies discuss specific components of the company's cybersecurity program, which most prominently include references to identity and access management, logging and monitoring, penetration testing and vulnerability scanning, governance, risk assessment and threat intelligence, employee awareness and training, and security monitoring. Companies also widely note where employees are provided with cybersecurity training (84%), with 27 of those companies disclosing that they provide this training on at least an annual basis.

- **Incident Response Preparedness.** The substantial majority of companies note the implementation of an incident response plan or procedures (87%), and nearly all companies (96%) describe the use of audits, drills, and/or tabletop exercises to test incident preparedness and the company's incident response processes.

In addition to the general requirement quoted above, Item 106(b)(1) includes a non-exclusive list of disclosure items, which most surveyed companies specifically address in their Item 1C disclosures as follows:

- **Whether and how any such processes have been integrated into the company's overall risk management system or processes**. In response to this disclosure item, a substantial majority of surveyed companies (90%) disclose that the oversight of cybersecurity risk has been integrated into the company's overall risk management system or processes.

- **Whether the registrant engages assessors, consultants, auditors or other third parties in connection with any such processes.** Nearly all companies (98%) generally disclose the engagement of assessors, consultants, auditors or other third parties in the management of cybersecurity risks. Most companies do not specifically name the third parties they engage.

- **Whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.** In line with Item 106's requirements, all companies generally discuss third-party risk management practices, including outlining processes for identifying and managing material cyber risks associated with third-party service providers. Ninety percent report evaluating, monitoring or conducting due diligence on a vendor's cybersecurity practices, and 42% report requiring vendors to adhere to certain cybersecurity management processes. These third-party risk management processes can range from conducting due diligence of the third party's information security environments, or reviewing their incident response capabilities, to monitoring their regulatory compliance to assess the company's own risk of exposure.

b. Cybersecurity Governance

Item 106(c)(1) requires that companies describe the role of the board in the oversight of cybersecurity risks, including the role of board committees or subcommittees, and Item 106(c)(2)(i) requires that companies describe the management's role in assessing and managing their material risks from cybersecurity threats, including addressing which management positions or committees are responsible for assessing and managing such risks. In response to these disclosure requirements, some of the most commonly addressed topics are as follows:

- **The Role of the Board and Committees of the Board in Cybersecurity Governance.** As part of the discussion of cybersecurity governance, a majority of surveyed companies (68%) report that the board is responsible for enterprise-wide risk oversight, which includes cybersecurity. However, a majority of companies (66%) also disclose that a committee or subcommittee of the board has been delegated responsibility for primary oversight of cybersecurity risks, with a minority of companies (28%) reporting that the board and a designated committee share the primary oversight of cybersecurity risks, and

a handful of companies (6%) reporting that the full board retains primary oversight of cybersecurity risks. Of the companies that delegate primary oversight of cybersecurity risks to a committee or subcommittee, or for which the board and a designated committee or subcommittee share oversight, companies most often disclose that the audit committee (78%) has this responsibility, followed by a risk committee (19%) (for companies that have a risk committee).

- **The Role of Management in Cybersecurity Governance.** In responding to this disclosure item, nearly all companies (99%) list one or more management positions responsible for addressing and managing cybersecurity risks, with a significant minority of companies (43%) reporting that a management committee is also responsible for managing such risks. Of the companies that identify a management position responsible for assessing and managing material cybersecurity risks, 61% identify one officer who fulfils this role and 39% identify more than one officer responsible for fulfilling this role. The substantial majority of companies (78%) identify a Chief Information Security Officer (CISO) among the management positions responsible for assessing and managing cybersecurity risks, while a minority of companies identify other positions, such as a Chief Information Officer (CIO) (14%), Chief Technology Officer (CTO) (4%), or another officer, such as a Chief Security Officer, Head of Technology, Chief Information and Digital Officer, and/or Chief Cybersecurity Officer.

Item 106(c)(2)(i) also requires a description of the relevant expertise of management in "such detail as necessary to fully describe the nature of the expertise." In response, a substantial majority of companies (88%) disclose the experience and/or qualifications of the individual(s) responsible for assessing and managing cybersecurity risk. While companies vary widely with respect to the level of specificity they provide in describing relevant experience or qualifications of those in management, surveyed companies generally provide examples of an individual's:

- **Roles and Positions Prior to Joining the Company.** Practice on this point varies widely, ranging from the inclusion of a general note stating that the individual has held various cybersecurity-related roles, to identifying the specific title held by such individual in the past roles, to noting the technical and industry-specific experience gained or skills employed in prior positions.
- **Years of Relevant Work Experience.** Where surveyed companies disclose this point, the years of experience range from 15 years to more than 30 years of relevant work experience.
- **Education and Certifications.** While less common than the other two categories mentioned above, some companies include reference to an individual's educational background or certifications (e.g., where the individual received certification as an information systems security professional (CISSP)).

Item 106(c)(2)(ii) requires that companies address how management is informed of and monitors the "prevention, detection, mitigation, and remediation of cybersecurity incidents." In response to this disclosure item, companies generally disclose that management is informed of cybersecurity risks and incidents through internal reporting channels, such as receiving reports from the company's cybersecurity professionals.

Item 106(c)(2)(iii) requires that companies discuss the process by which management reports cybersecurity risks to its board. In response to this disclosure item, all companies disclose that the board or responsible committee receives reports from management, with a substantial

majority of these companies (82%) disclosing that the board or responsible committee receives reports on a regular basis.[5] A majority of the surveyed companies (61%) also report a process for escalating certain cybersecurity incidents, risks or threats to the board or responsible committee.

c. Material Cybersecurity Risks, Threats & Incidents

Item 106(b)(2) requires that companies "[d]escribe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how." While disclosure on this point varied greatly, we observed the following trends among surveyed companies in response to this disclosure item:

- **Some Companies Did Not Affirmatively Address Item 106(b)(2) in Item 1C.** Twenty-two percent of surveyed companies do not appear to have included disclosure responsive to Item 106(b)(2) in Item 1C.[6] Of these companies, 90% provide a cross-reference to a discussion in Item 1A "Risk Factors."[7]
- **Most Disclosures Track the Language of Item 106(b)(2).** Forty percent of surveyed companies largely track the language of the disclosure item with respect to both the backward-looking aspect ("have materially affected") and the forward-looking aspect ("are reasonably likely to materially affect") of the rule by responding in the negative, concluding that they did not identify any risks from cybersecurity threats that have materially affected or are reasonably likely to materially affect the company, including its business strategy, result of operations or financial condition. However, the precise formulation varied from company to company.[8] Of these companies:
    - 54% include a knowledge qualifier making clear that they are "not aware" or "do not believe" that such risks have materially affected or are reasonably likely to materially affect the company;
    - 67% make clear that they are speaking as of the end of the fiscal year covered by the Form 10-K or as of the date of the Form 10-K;
    - in addition to tracking the rule, 44% include a disclaimer noting that there is no "guarantee" or "assurance" (or something similar) that cyber-related risks may not be material in the future;
    - 26% limit required disclosure to threats identified during the last year or last three fiscal years; and
    - one company limited the future horizon to "over the long term."
- **Many Companies Vary Disclosure on Forward-Looking Impacts, or Address It Vaguely or Not At All.** Thirty-eight percent of surveyed companies address the backwards-looking aspect of the rule by largely tracking the rule on that point. For the forward-looking aspect of the rule, some of them: (i) simply do not address it at all or make vague references to potential future impacts (35%); (ii) include a disclaimer noting that there is no "guarantee" or "assurance" (or something similar) that cyber-related risks may not be material in the future (51%); or (iii) make explicit what is an inherent assumption in the disclosure requirement, such as by stating that risks from cybersecurity threats, "if realized," are reasonably likely to materially affect business strategy, results of operations, or financial condition (16%). One company includes both a "no guarantee"

disclaimer and "if realized" language (3%). In addition, among these 38% of the surveyed companies:

- 16% include a knowledge qualifier making clear that they are "not aware" or "do not believe" that such risks have materially affected the company;
- 41% make clear that they are speaking as of the end of the fiscal year covered by the Form 10-K or as of the date of the Form 10-K; and
- 27% limit required disclosure to threats identified during the last year, last three fiscal years or "recent years."

IV. ISS Governance QualityScore[9]

While it is not possible to say definitively, it is possible that some of the reporting trends observed among the surveyed companies may be attributable to the questions included by Institutional Shareholder Services ("ISS") in its Governance QualityScore ("QualityScore") relating to information security since they are not otherwise directly responsive to Item 106 requirements. For example:

- possibly in response to **ISS Question 409**, which evaluates disclosure regarding whether the company has information security risk insurance, a minority of surveyed companies (26%) disclose maintaining some level of cybersecurity insurance;
- possibly in response to **ISS Question 405**, which assesses disclosure as to how many directors have information security skills, a minority of companies (14%) report having directors with information security experience, despite the fact that the proposed requirement to disclose this information was not included in the final cybersecurity rule;[10] and
- possibly in response to **ISS Question 407**, which assesses whether a company experienced an information security breach in the last three years, 3% of companies frame their statements about material effects from cybersecurity threats or incident using this specific time period.

V. Drafting Considerations

The majority of surveyed companies (66%) divide their disclosure into two sections tracking the organization of Item 106, with one section dedicated to cybersecurity risk management and strategy and another section focused on cybersecurity governance. Of those companies, 33% include subsections within one or both of those two main sections, 23% of surveyed companies use no headings at all, and 11% of surveyed companies use headings that differ from the structure of Item 106 (either by including more than the two primary sections set forth in the rule or by including distinct headings altogether).

The average length of disclosure among surveyed companies is 980 words, with the shortest disclosure at 368 words and the longest disclosure at 2,023 words. The average disclosure runs about a page and a half.

VI. Comment Letters

As of November 30, 2024, there have been five comment letters from the Staff regarding disclosure under Item 1C. While these comment letters have not been issued in response to disclosure in annual reports on Form 10-K filed by the S&P 100 companies we surveyed, we are including a discussion of them here for completeness, as they are instructive as to what the Staff was focused on when reviewing the first set of Item 106 disclosures. To summarize:

- Two of these comment letters simply requested that companies refile their annual reports on Form 10-K to include an omitted Item 1C.[11] In both instances, the companies filed an amendment on Form 10-K/A, adding the requested disclosure.[12]
- One comment letter requested that a company amend future filings to clarify inconsistent statements about its engagement of third parties in connection with its processes for identifying, assessing and managing material risks from cybersecurity threats.[13] The company responded by clarifying the nature of its engagement of third parties in identifying and managing cybersecurity risks, and also confirmed that it would clarify this point to avoid any inconsistency or ambiguity in future filings.[14]
- In three comment letters, the Staff touched upon the following requirements of Item 106, requesting expanded disclosure in future filings:
    - **Item 106(b)(1) (*Processes for Assessing, Identifying, and Managing Material Risk from Cybersecurity Threats*).** The Staff requested that a company expand its disclosure to describe the areas of responsibility of its executive management team and board of directors, along with their respective processes in response to this disclosure item.[15] The company responded by confirming it would include the requested detail in future filings.[16]
    - **Item 106(b)(1)(i) (*Integration of Cybersecurity Risk Processes into Overall Risk Management*).** In one comment letter, the Staff requested that a company revise future filings to disclose how processes for "assessing, identifying, and managing" material cybersecurity threats have been integrated into its overall risk management system or processes in response to this disclosure item.[17] The company responded by emphasizing that these processes are "well integrated" into its overall risk management system, noting relevant disclosure included in its current filing, and agreeing to provide more detail in future filings in response to this disclosure item.[18]
    - **Item 106(c)(2)(i) (*Identification of Management Committees or Positions Responsible for Assessing and Managing Material Risks from Cybersecurity Threats*).** Two of the comment letters noted above also included comments related to the discussion of management's responsibility over cybersecurity risks. The first comment letter requested the company identify which management positions or teams are responsible for assessing and managing material risks from cybersecurity threats in future filings.[19] The second such letter requested a discussion of the relevant expertise of the company's senior leadership responsible for managing the company's cybersecurity risk and the "design and implementation of policies, processes and procedures to identify and mitigate this risk."[20] In each case, the company responded by confirming it would include the requested detail in future filings.[21]

While the impact of the November 2024 election on future leadership of the SEC is uncertain, as are their strategic and enforcement priorities, we expect SEC scrutiny over cybersecurity incident disclosures to continue as companies adjust their disclosure practices to the new requirements.

VII. XBRL Requirements

As a reminder for the upcoming Form 10-K season, all Item 106 disclosures must be tagged in Inline XBRL (block text tagging for narrative disclosures and detail tagging for quantitative amounts) beginning one year after the initial compliance date of December 15, 2023, which, for most companies, means starting with their Form 10-K or Form 20-F filed in 2025.

Companies must use the "Cybersecurity Disclosure (CYD)" taxonomy tags within iXBRL to tag these disclosures.[22] We note that significant judgment will be required to apply these tags. Not only will companies be required to determine the provision of Item 106 to which each part of the narrative disclosure is responsive, but companies will need to determine which flags to mark as "true" or "false." Importantly, there is a flag for "Cybersecurity Risk Materially Affected or Reasonably Likely to Materially Affect Registrant [Flag]" and, it is our understanding that to properly apply the flag, each company must select "true" or "false." Companies that have addressed Item 106(b)(2) by including slightly vague or ambiguous disclosure in Item 1C or by cross-referencing their risk factors will need to carefully consider how they will handle these new tagging requirements.

[1] This alert memo highlights certain disclosure trends based on our review of the 97 surveyed companies. (As of November 30, 2024, three S&P 100 companies had not yet filed annual reports on Form 10-K for fiscal years ending on or after December 15, 2023.) Where appropriate, we have grouped together similar responses to disclosure items to enable a comparison among the companies' disclosures. For example, where a company provided time qualifiers such as "in the last year," "in 2023," or "during the last fiscal year," we have considered these to be similar data points in our survey of company disclosures. Percentages may not add up to 100% due to rounding.

[2] Foreign private issuers are required to make similar annual disclosures pursuant to Item 16K of Form 20-F.

[3] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216 (July 26, 2023) ("Adopting Release") at 60-63.

[4] Companies are wise to be cautious when describing their adherence to cybersecurity frameworks and standards, as underscored by the SEC's recent enforcement action against SolarWinds Corporation where the SEC charged the company with making a materially misleading statement when it claimed "SolarWinds follows the NIST Cybersecurity Framework" despite internal assessments showing that most NIST controls were not met. *See SEC v. SolarWinds Corp.*, 1:23-CV-09518 (S.D.N.Y. July 18, 2024), at 11-14.

[5] In counting the companies who disclose where management reports to the board or responsible committee on a regular basis, we have included companies that state that they do this "regularly" (e.g., regularly, "at each regularly scheduled meeting," etc.), as well as companies

who refer to a specific time period (e.g., annually, quarterly, semi-annually, mid-year, etc.). This does not include where companies use language such as “periodically,” “as appropriate,” “as necessary,” or “as needed.”

[6] Our review of company cybersecurity disclosure was limited to the language included in Item 1C. We have not reviewed other sections of Forms 10-K filed by surveyed companies to determine whether they contain disclosure that can be deemed responsive to Item 106(b)(2).

[7] We have not reviewed the cross-referenced risk factor, or the risk factors section more generally, to determine whether they contain disclosure that can be deemed responsive to Item 106(b)(2).

[8] The language surveyed companies use to disclose how they have been impacted by cybersecurity risks, threat, or incidents is imprecise. For example, some companies specifically discuss the effect of cybersecurity incidents, while others fully track the language of the rule and discuss “risks from cybersecurity threats”.

[9] On October 28, 2024, ISS announced an update to its ISS QualityScore product to include 12 new factors. Among these are the following Audit and Risk Oversight factors related to cybersecurity risk management:

- **Question 460.** Does the company disclose the role of the management in overseeing information security risks?
- **Question 461.** Does the company disclose the role of the board in overseeing information security risks?
- **Question 462.** Does the company have a third-party information security risk management program?
- **Question 463.** Does the company leverage a third-party assessment of information security risks?
- **Question 464.** What is the Data Protection Officer reporting line?

These factors generally align with the disclosure requirements under the rule, and based on our survey results, companies are already addressing Questions 460-463 while preparing their Item 106 disclosures.

[10] Adopting Release, *supra* note 3, at 81-85.

[11] *See* SEC Comment Letter to Quarta-Rad, Inc. dated August 1, 2024; SEC Comment Letter to Scientific Industries, Inc. dated June 14, 2024.

[12] *See* Response Letter from Quarta-Rad, Inc. to the SEC dated August 15, 2024; Response Letter from Scientific Industries, Inc. to the SEC dated July 17, 2024.

[13] *See* SEC Comment Letter to Wilhelmina International, Inc. dated August 21, 2024 ("SEC Letter to Wilhelmina International").

[14] *See* Response Letter from Wilhelmina International, Inc. to the SEC dated September 3, 2024 ("Wilhelmina International Response Letter").

[15] *See* SEC Comment Letter to TNF Pharmaceuticals, Inc. dated September 23, 2024 ("SEC Letter to TNF Pharmaceuticals"). In its comment letter, the Staff noted that the responsive disclosure needed to be in sufficient detail for a reasonable investor to understand.

[16] *See* Response Letter from TNF Pharmaceuticals, Inc. to the SEC dated September 30, 2024 ("TNF Pharmaceuticals Response Letter").

[17] *See* SEC Comment Letter to Blackbaud, Inc. dated August 23, 2024.

[18] *See* Response Letter from Blackbaud, Inc. to the SEC dated September 3, 2024.

[19] SEC Letter to TNF Pharmaceuticals, *supra* note 15.

[20] SEC Letter to Wilhelmina International, *supra* note 13.

[21] Wilhelmina International Response Letter, *supra* note 14; TNF Pharmaceuticals Response Letter, *supra* note 16.

[22] *See* the Cybersecurity Disclosure Taxonomy Guide (September 16, 2024), available at https://www.sec.gov/data-research/standard-taxonomies/operating-companies.

Please click below to view the complete update and endnotes on Gibson Dunn's website:

Read More

The following Gibson Dunn lawyers assisted in preparing this update: Thomas Kim, Julia Lapitskaya, Michael Titera, Stephenie Gosnell Handler, Vivek Mohan, Alexandria Johnson, Isaac Maycock, and Kayla Jahangiri.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these developments. To learn more, please contact the Gibson Dunn lawyer with whom you usually work in the firm's Securities Regulation & Corporate Governance or Privacy, Cybersecurity & Data Innovation practice groups, the authors, or any of the following practice leaders and members:

Securities Regulation & Corporate Governance:
Elizabeth Ising – Co-Chair, Washington, D.C. (+1 202.955.8287, eising@gibsondunn.com)
James J. Moloney – Co-Chair, Orange County (+1 949.451.4343, jmoloney@gibsondunn.com)
Lori Zyskowski – Co-Chair, New York (+1 212.351.2309, lzyskowski@gibsondunn.com)
Aaron Briggs – San Francisco (+1 415.393.8297, abriggs@gibsondunn.com)
Thomas J. Kim – Washington, D.C. (+1 202.887.3550, tkim@gibsondunn.com)
Brian J. Lane – Washington, D.C. (+1 202.887.3646, blane@gibsondunn.com)
Julia Lapitskaya – New York (+1 212.351.2354, jlapitskaya@gibsondunn.com)
Ronald O. Mueller – Washington, D.C. (+1 202.955.8671, rmueller@gibsondunn.com)
Michael Scanlon – Washington, D.C.(+1 202.887.3668, mscanlon@gibsondunn.com)
Michael A. Titera – Orange County (+1 949.451.4365, mtitera@gibsondunn.com)

Privacy, Cybersecurity & Data Innovation:
Ahmed Baladi – Co-Chair, Paris (+33 1 56 43 13 00, abaladi@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com)
Joel Harrison – Co-Chair, London (+44 20 7071 4289, jharrison@gibsondunn.com)
Jane C. Horvath – Co-Chair, Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com)
Rosemarie T. Ring – Co-Chair, San Francisco (+1 415.393.8247, rring@gibsondunn.com)
Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com)
Vivek Mohan – Palo Alto (+1 650.849.5345, vmohan@gibsondunn.com)
Sophie C. Rohnke – Dallas (+1 214.698.3344, srohnke@gibsondunn.com)