wiley

ARTICLE

NIST Plays Increasingly Prominent Role in Privacy Policy

Law360
March 12, 2015

A technical agency within the Department of Commerce is poised to have a substantial impact on American businesses, through efforts on cybersecurity, data security, and privacy. The National Institute of Standards and Technology has taken a leadership role on technology issues by producing guidance documents that are broad in scope and may influence regulatory agendas and expectations about private sector operations and policies. The private sector should be engaged and watchful, as NIST's work generally is not bound by notice and comment procedures and is rarely subject to judicial review, but could become *de facto* obligations or expectations for private behavior.

NIST Produces Guidance and Standards by Consensus, Outside Familiar Administrative Law Procedures

NIST, housed within the U.S. Department of Commerce, is a non-regulatory agency. [1] Since its inception in 1901, [2] the agency has been charged with, among other things, "stimulating cooperative work among private industrial organizations in efforts to surmount technological hurdles." [3] NIST's stated mission is to "[t]o promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." [4] NIST has core responsibilities under the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541 *et seq.,* Public Law 107-347, "for developing information security standards and guidelines, including minimum requirements for federal information systems." [5]

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Media
Privacy, Cyber & Data Governance
Telecom, Media & Technology

NIST performs several functions, including developing standards and guidelines for federal information systems; [6] supporting Commerce in facilitating trade; [7] and cooperating in international- and private-efforts to establish standard practices and voluntary, consensus-based standards. [8] Much of NIST's work is spread among six internal research laboratories, including the Information Technology Laboratory (ITL). [9]

In carrying out its functions, NIST publishes a variety of guidance, including handbooks, NIST interagency or internal reports (NISTIRs), special publications, technical notes, and bulletins, among others. [10] "While developed for federal agency use, these resources are voluntarily adopted by other organizations because they are effective and accepted throughout the world." [11] NIST's work has been influential in government procurement policy by, for example, setting security standards for federal contractors and others that store controlled unclassified information (CUI) on their systems.

NIST is a non-regulatory agency and its procedures are often unlike the notice-and-comment procedures of regulatory agencies dictated by the Administrative Procedures Act (APA). In some instances, NIST will follow procedures "modeled after" the APA[12], but for other work, such as special publications, NIST tends toward the creation of voluntary, consensus-based standards [13] via workshops and meetings rather than formal rulemakings. NIST explains that "standards and guidelines are developed in an open and transparent manner that enlists broad industry and academia expertise from around the world." [14] NIST's development of the *Framework for Improving Critical Infrastructure Cybersecurity*, discussed below, illustrates the collaborative, workshop-based approach NIST often uses. NIST's substantive work is not often subject to judicial review [15], though its efforts often are used by other agencies as a standard or benchmark.

The legal impact of NIST guidance and expertise outside the federal government is not well developed [16], but NIST's work has been used in a variety of ways by courts and litigants. NIST studies and standards have been cited by litigants and analyzed by courts in cases concerning products liability [17], patent infringement [18] and false advertising. [19]

Litigants also cite NIST guidance in their advocacy. For example, NIST's activities were raised in a key case challenging the Federal Trade Commission's authority to regulate data security. In *FTC v. Wyndham Worldwide Corporation*, a federal court upheld the FTC's authority to bring an enforcement action against a hotel company for failing to use reasonable and appropriate data security practices. [20] There, Wyndham and amici had argued that the FTC could not develop or enforce general data security standards, and cited NIST's then-pending Framework efforts as an example of appropriate standard-setting. [21]

NIST Is a Leader on Data Security, Privacy and Cybersecurity

NIST supports federal network security standards, guidelines, and best practices. [22] Its work feeds into national and international consensus standards, and informs state and local governments, along with private industry. [23]

Of late, NIST has been taking on an increasingly high profile on issues related to privacy and security, principally through its ITL, which "has the broad mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and

development in information technology, mathematics, and statistics." [24] The ITL contains the Computer Security Division (CSD), which is responsible for developing standards, guidelines, tests, and metrics for the protection of non-national security federal information and communications infrastructure. CSD includes the Computer Security Resource Center, which facilitates "sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia."

As shown in a recent Annual Report, the CSD is addressing a variety of issues, as diverse as smart-grid cybersecurity, health information technology security, supply chain risk management, cloud computing, and identity verification. NIST is proud of its role in developing "scalable and sustainable information security standards and practices in areas such as cyber-physical and industrial control systems, privacy engineering, security automation, and mobile technologies." [25] These areas are all emerging as major challenges for government and the private sector.

NIST has taken a lead role in federal cybersecurity efforts, and is impacting regulatory activities throughout the federal government.

In February 2013, President Obama issued an Executive Order (EO) on Improving Critical Infrastructure (CI) Cybersecurity. [26] The EO tasked NIST with developing a voluntary cybersecurity framework through an open, consultative process. To implement its responsibilities under the EO, NIST held several open planning sessions for the voluntary cybersecurity framework during 2013-2014. NIST released a proposed framework, on which it accepted comments from interested parties, and finalized the framework in February 2014. [27]

The framework provides broad cybersecurity guidance using a risk-based approach that can be adapted to the needs of different CI sectors. It consists of three parts: the core, profile and implementation tiers. The *core* is a set of activities and outcomes NIST found applicable to all CI sectors. It is organized into five functions-identify, protect, detect, respond, and recover-that are recognized components of a cybersecurity management lifecycle, along with associated programmatic and technical outcomes. The profiledescribes an entity's current and target cybersecurity postures, based on business needs. And the implementation tiers characterize an entity's current and intended practices. The framework is not intended to be mandatory or static, and NIST explicitly states that it can updated.

Industry has been generally supportive of NIST's efforts on the cybersecurity framework, in particular the agency's open and collaborative approach, and its commitment to keep the resulting Framework voluntary and non-regulatory. [28]

NIST's cybersecurity activities are influencing initiatives at other government agencies:

- The Food and Drug Administration incorporated the framework into recent guidance related to cybersecurity on medical devices. [29]
- The National Highway Traffic Safety Administration is using the framework to analyze cybersecurity risk management in the automotive sector. [30]

- The Securities and Exchange Commission's Office of Compliance Inspections and Examinations has undertaken a cybersecurity initiative that includes conducting examinations of registered broker-dealers and registered investment advisors focused, among other things, on identification and assessment of cybersecurity risks and protection of networks and information. [31] The inquiry largely tracks the framework. [32]
- The Federal Trade Commission, which has asserted broad authority over private sector data security issues, will consider the framework in its data security activities and investigations. [33]
- The Federal Communications Commission's Communications Security, Reliability, and Interoperability Council is looking at mechanisms to provide macro-level assurance that communications providers are reducing cybersecurity risks through the application of the framework, or an equivalent construct. [34]
- The Department of Defense and the General Services Administration used the framework in its development of cybersecurity guidelines for government acquisition. [35]

Future government cybersecurity initiatives are expected to rely on or refer to the framework, and may look to NIST for guidance and standards in related areas.

As a result of its perceived success in handling its responsibilities under the EO, policy makers have codified NIST's inclusive public-private, technology-neutral approach to the framework. The Cybersecurity Enhancement Act of 2014, signed into law in December 2014, amends the National Institute of Standards and Technology Act to reflect NIST's leadership and ensure that the framework continues to be a voluntary, consensus-based, industry-led set of standards and procedures to cost-effectively reduce cyber risks to critical infrastructure. [36]

That legislation envisions a leading role for NIST. It requires the NIST director to identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted by owners and operators of CI to help identify, assess, and manage cyber risks. The approach must mitigate impacts on business confidentiality, protect individual privacy and civil liberties, incorporate voluntary consensus standards and industry best practices, align with international standards, and prevent duplication of regulatory processes.

NIST is to coordinate with the private sector, CI owners and operators, sector coordinating councils, Information Sharing and Analysis Centers, and other relevant industry organizations. NIST also must consult with the heads of agencies with national security responsibilities, sector-specific agencies, state and local governments, governments of other nations, and international organizations. [37] The law prohibits NIST from prescribing a specific solution or requiring that products or services be designed or manufactured in a particular manner[38], but its guidance and effort promises to be influential.

NIST is addressing many privacy and security issues affecting the private sector.

NIST's work on security and privacy can be expected to continue and expand, both as it relates to the President's EO on cybersecurity, and more broadly.

NIST is examining a variety of additional issues as it implements the EO on cybersecurity. NIST has identified for additional study numerous topics, including authentication, automated sharing of indicators, assessment of the degree of conformity to risk-management requirements, cybersecurity workforce needs, data analytics, supply-chain risk management, technical standards relating to privacy, alignment of the framework with federal agency cybersecurity requirements, and international aspects and implications. [39] And, NIST has been exploring other aspects of cybersecurity, which could impact the private sector. For example, in a recent effort, NIST has been examining information-sharing architectures. [40] Each of these areas is complex, and the reach of NIST's activities could be broad.

NIST's work is not limited to the cybersecurity framework and closely related activities. NIST has been addressing privacy and security broadly, and for multiple audiences. For example, it offers guidance on small business information security in partnership with the Small Business Administration and the FBI. [41] The guidance's goal is to present the fundamentals of small business information security in non-technical language, and it refers to the cybersecurity framework throughout.

NIST is also addressing mobile security and applications. In January 2015 it released SP 800-163, *Vetting the Security of Mobile Applications*, which recognizes that the "use of apps can potentially lead to serious security risks" and is "intended for organizations that plan to implement an app vetting process or leverage existing app vetting results from other organizations. It is also intended for developers that are interested in understanding the types of software vulnerabilities that may arise in their apps during the app's software development life cycle." [42] In the past, NIST has addressed mobile device security, including in a Draft Publication, SP 800-164, *Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)*. [43]

In addition, NIST is looking at broad and evolving privacy issues. For example, NIST's ITL is in the midst of an effort aimed at advancing privacy engineering as a basis for the development of technical standards, guidelines, and best practices for the protection of individuals' privacy and civil liberties. NIST seeks to develop objectives and a risk model for privacy engineering, with an eye toward developing controls and metrics as part of a privacy engineering standard. NIST's inquiry may result in guidance that would be applicable across government, and informative to the private sector. Some in the private sector have urged NIST to proceed with caution, given the lack of existing, general privacy policy norms that would inform its selection of objectives. NIST has stated that its effort aims to identify best practices, but industry has voiced concern about NIST's broader approach, which some fear may pull the agency into substantive policy questions about privacy.

Because NIST Activities May Drive Compliance Concerns and Operational Norms, the Private Sector Should Be Engaged

The private sector should be mindful of NIST's increasing leadership in security and privacy. While lawmakers and agencies grapple with difficult technical and policy questions, NIST is providing a source of generally applicable guidance on a variety of issues. And, even where it is explicitly intended to be non-binding and voluntary, NIST's work may turn out to be a platform for future regulatory obligations or standards of care. At a minimum, NIST's work is informative of government procurement efforts, [44] and can be expected to turn up

in government contracting in various ways.

NIST's cybersecurity and privacy work may not be a suitable basis for regulatory expectations. Scholars have identified hard questions about when and how third party standards are appropriate foundations for regulatory action. [45] Best practices that are process-based, voluntary, or conditional can be poor candidates for incorporation into regulation. And, many approaches have been designed by NIST for use by the federal government, making their application to the private sector questionable. [46] Finally, despite effort by NIST to be open and inclusive, not all activities are broadly subject to regular administrative process.

Notwithstanding these concerns, in the absence of something more suitable, agencies and courts may rely on NIST's work. Agencies across the government are looking to the cybersecurity framework to inform regulatory oversight, and they can be expected to incorporate NIST's expertise and guidance into various activities. And, separate from regulatory action, NIST's activities on security and privacy may shape-or become-standards of care for the private sector, through private litigation or otherwise. As noted, the defendants in *Wyndham* cited to the NIST framework, implying that it might represent the sort of regulatory expectation that the FTC was lacking when it brought its enforcement action against Wyndham. [47]

Industry has been urging NIST to include clear statements about the scope and applicability of its work. But, without federal rules or applicable technical and operational standards, NIST's work is poised to take on increasing importance to the private sector.

---

[1] *See* NIST, General Information, *available at http://www.nist.gov/public_affairs/general_information.cfm ;* Dismas N. Locaria, Andrew Bigart, & Keir Bancroft, *NIST's Proposed Cybersecurity Research and Development Center*, 27 No. 7 Westlaw J. Gov. Contract 1 (Aug. 5, 2013).

[2] The agency was originally founded as the National Bureau of Standards. *See* National Bureau of Standards Organic Act, P.L. 56-177, as amended, 15 U.S.C. § 271 *et seq.*; *see also* James F. Schooley, NIST Special Publication 955, *Responding to National Needs: The National Bureau of Standards Becomes the National Institute of Standards and Technology 1969-1993,* 614-15 (2000), *available at* http://www.nist.gov/nvl/nist-nbs_history.cfm. In 1988, Congress modernized and restructured the agency, giving it its current name. *See* Omnibus Trade and Competitiveness Act of 1988, P.L. 100-418 (1988).

[3] 15 U.S.C. § 271(a)(5); *see also* Schooley at 615 ("Efforts need to be focused through a designated entity that can effectively respond to industry initiatives and interact with non-government groups, including industry. ").

[4] NIST, Mission, Vision, Core Competencies, and Core Values, *available at* http://www.nist.gov/public_affairs/mission.cfm.

[5] *See* NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, ii, Authority (Apr. 2013) (describing source and scope of agency authority), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[6] 15 U.S.C. § 278g-3; *see also* Marianne Swanson, Joan Hash, & Pauline Bowen, NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems* iii (2006) ("NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems."), *available at* http://csrc.nist.gov/publications/PubsSPs.html.

[7] Congress has tasked NIST with "helping U.S. industry increase its competitiveness in the global market place." U.S. Dep't of Commerce, *Accelerating Technology Transfer and Commercialization of Federal Research in Support of High-Growth Businesses* 3 n.1 (Sept. 2012), *available at* http://www.nist.gov/tpo/publications/upload/DOC-Tech-Transfer-Plan.pdf.

[8] 15 U.S.C. § 272(b)(10).

[9] *See* Wendy T. Schacht, Congressional Research Service, *The National Institute of Standards and Technology: An Appropriations Overview* (Nov, 20, 2013).

[10] For a full list of NIST publications *see* http://www.nist.gov/nvl/nist_series_publications.cfm.

[11] NIST, Computer Security Division 2013 Annual Report 1 (2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-170.pdf ("CSD 2013 Annual Report").

[12] For example, NIST's work on Federal Information Processing Standards (FIPS) is published in the Federal Register and subjected to a comment cycle. *See* NIST, Information Technology Lab, General Information ("Federal Information Processing Standards (FIPS), the National Institute of Standards and Technology follows rule-making procedures modeled after those established by the Administrative Procedures Act."), available at http://www.nist.gov/itl/fipsinfo.cfm

[13] *See id.* ("In accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113) and Administration policies, NIST supports the development of voluntary industry standards both nationally and internationally as the preferred source of standards to be used by the Federal government.")

[14] CSD 2013 Annual Report at 1. NIST does, however, seek public comment on many of its publications. *See, e.g.* NIST, Drafts, Computer Security Division Computer Security Resource Center Publications (seeking public comment on a number of drafts of computer security publications, including FIPS, Special Publications, and NISTIRs), *available at* http://csrc.nist.gov/publications/PubsDrafts.html.

[15] NIST's technical guidance and publications are not the sort of final agency action ordinarily subject to judicial review. Other decisions can lead to judicial review. *See Raitport v. National Bureau of Standards*, 378 F. Supp. 380, 385 (E.D. Pa. 1974) (holding that a National Bureau of Standards decision to reject a proposal was subject to judicial review).

[16] *See In re Pilgrim's Pride Corp.*, No. 08-45664, 2011 WL 3799835, n.23 (Bankr. N.D. Tex. Aug. 26, 2011) (noting that even though NIST's weights and measures standards are not *per se* legally binding, many states incorporate the standards into state laws).

[17] *See, e.g., In re Nissan North America, Inc. Odometer*, 664 F. Supp. 2d 873, 891 (M.D. Tenn. 2009) (rejecting defendants' reliance on a NIST odometer standard adopted in California because plaintiffs' allegation went beyond odometer accuracy); *Kearney v. Philip Morris, Inc.*, 916 F. Supp. 61, 66-69 (D. Mass. 1996) (refusing to give weight to plaintiff's product defect theory based on a NIST study because the theory was based on "an inferential leap for which no reasoned basis [wa]s proffered").

[18] *ProChroma Techs., Inc. v. United States*, 60 Fed. Cl. 614, 626 & n.26 (2004).

[19] *Kwan Software Engineering, Inc. v. Foray Techs., LLC*, No 12-03762, 2013 WL 244999, at *7 (N.D. Cal. Jan. 22, 2013).

[20] 10 F. Supp. 3d 602 (D.N.J. 2014).

[21] *See* Defendant's Motion to Dismiss, *FTC v. Wyndham Hotels & Resorts LLC*, No. 13-cv-1887, 2013 WL 345984 (D.N.J. Apr. 26, 2013); Brief Amicus Curiae of the International Franchise Association in Support of Defendant's Motion to Dismiss, *FTC v. Wyndham Hotels & Resorts LLC*, No. 13-cv-1887, 2013 WL 3739748 (D.N.J. May 3, 2013).

[22] *See* Testimony of Cita M. Furlani, Director, Information Technology Laboratory, NIST, *Hearing Before the Subcomm. on Technology & Innovation of the H. Comm. on Science & Technology* (Oct. 22, 2009), *available at* http://www.nist.gov/director/ocla/testimony/upload/cfurlani_nist_cybersecurity_testimony102209.pdf.

[23] *See id.*

[24] NIST, Information Technology Laboratory, *What ITL Does*, *available at* http://www.nist.gov/itl/what-itl-does.cfm.

[25] CSD 2013 Annual Report at 2.

[26] Executive Order 13636 - Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013) (EO), *available at* http://www.whitehouse.gov/the-press-office/2013/12/executive-order-improving-critical-infrastructure-cybersecurity. The President simultaneously released a Presidential Policy Directive on Critical Infrastructure Security and Resilience which elaborates on the goals of the EO. *See* Presidential Policy Directive 21- Critical Infrastructure Security and Resilience (Feb. 12, 2013) (PPD), *available at*http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. The EO provides for expanding information sharing and collaboration between the government and the private sector; developing of a voluntary framework of cybersecurity standards and best practices for protecting CI; establishing a consultative process for improving CI cybersecurity; identifying CI with especially priority for protection using the consultative process; establishing a program with incentives for voluntary adoption of the framework by CI owners and operators; reviewing cybersecurity regulatory requirements to determine if they are sufficient and appropriate; and incorporating privacy and civil liberties protections in activities under the order.

[27] NIST, Framework for Improving Critical Infrastructure Cybersecurity, v. 1.0 (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[28] *See, e.g.*, Comments of CTIA, *Experience with the Framework for Improving Critical Infrastructure Cybersecurity*, Docket No. 140721609-4609-01 (Oct. 10, 2014), *available at* http://www.ctia.org/docs/default-source/fcc-filings/ctia-response-rfi-nist-framework10102014.pdf?sfvrsn=0.

[29] FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff (Oct. 2, 2014), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.

[30] NHTSA, DOT HS 812 073, National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles (Oct. 2014), *available at* http://www.nhtsa.gov/Research/Crash+Avoidance/Vehicle+Cybersecurity.

[31] SEC, National Exam Program Risk Alert, OCIE Cybersecurity Initiative, Vol. IV, Issue 2 (Apr. 15, 2014), *available at* http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

[32] *Id.*, Appendix 1.

[33] *See, e.g.*, FTC Commissioner Julie Brill, *Keynote Address Before the Center for Strategic and International Studies "Stepping into the Fray: The Role of Independent Agencies in Cybersecurity"* (Sept. 17, 2014) (the NIST Framework is "fully consistent with the FTC's enforcement framework"), *available at* http://www.ftc.gov/system/files/documents/public_statements/582841/140917csisspeech.pdf.

[34] *See* CSRIC IV Working Group Descriptions and Leadership (updated Oct. 23, 2014), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC%20IV%20Working%20Group%20Descriptions%2010%2023%2014.pdf.

[35] *See* DoD and GSA, Improving Cybersecurity and Resilience through Acquisition (Nov. 2013), *available at* http://www.defense.gov/news/Improving-Cybersecurity-and-Resilience-Through-Acquisition.pdf.

[36] Cybersecurity Enhancement Act of 2014, P.L. 113-274 (Dec. 18, 2014).

[37] *Id.*

[38] *Id.*

[39] To assist in adoption and implementation of the framework by CI entities, DHS has developed the Critical Infrastructure Cyber Community C^3 Voluntary Program. Its goals are to help CIT entities understand and use the framework and obtain feedback from them on improvements.

[40] *See* Chris Johnson, Lee Badger & David Waltermire, *Guide to Cyber Threat Information Sharing (Draft),* NIST

Special Publication 800-150 (Draft) (Oct. 28, 2014), *available at* http://csrc.nist.gov/publications/drafts/800-

150/sp800_150_draft.pdf.

[41] NIST, *Small Business Information: The Fundamentals*, Draft NISTIR 7621 (Dec. 2014), *available at* http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir_7621_r1_draft.pdf.

[42] NIST, SP 800-163, *Vetting the Security of Mobile Applications* vi (Jan. 2015), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf.

[43] NIST, SP 800-164, *Guidelines on Hardware-Rooted Security in Mobile Devices* (Draft) (Oct. 2012), *available at http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf.*

[44] *See, e.g.,* Susan Cassidy and Catlin Meade, *NIST Draft Standards Provide Guidance for Protecting CUI on Contractor Systems*, InsideGovernmentContracts.com (Nov. 21, 2014), *available at* http://www.insidegovernmentcontracts.com/2014/11/nist-draft-standards-provide-guidance-for-protecting-cui-on-contractor-systems/.

[45] *See* Emily S. Bremer, *Incorporation by Reference in an Open-Government Age*, 36 Harv. J.L. & Pub. Pol'y 131, 202 (2013) (where federal regulators rely on or incorporate standards, the referenced standards must be specific and not phrased in a conditional manner because "agencies may confuse regulated parties by incorporating by reference material that is phrased as-and was intended by its drafter to be-nonregulatory."); *see also* Administrative Conference of the United States, Recommendation 2011-5 (2012) (providing guidance to agencies that seek to rely on technical standards in regulatory efforts).

[46] *See* Isaac Potoczny-Jones, *Is the NIST Risk Management Framework Poised to Become a National Cybersecurity Standard?*, gloois.com (Aug. 2, 2012), (noting that complexity of NIST Framework could make applicability to industry, particularly small businesses, challenging), *available at* http://galois.com/blog/2012/08/is-the-nist-risk-management-framework-poised-to-become-a-national-cybersecurity-standard/.

[47] *See* Defendant's Motion to Dismiss, *FTC v. Wyndham Hotels & Resorts LLC*, No. 13-cv-1887, 2013 WL 345984 (D.N.J. Apr. 26, 2013).