# Practical Impact of the Updates to the NIST Cybersecurity Framework

*Kent Bressie, Adrienne Fowler, Robert Friedman, and Michael Carlson*

The National Institute of Standards and Technology (NIST) recently released an update to its Framework for Improving Critical Infrastructure Cybersecurity, commonly known as the NIST Framework. The original version of the Framework (Version 1.0) was released in February 2014 and served as a widely used, voluntary roadmap for assessing and managing cybersecurity risks. The new version (Version 1.1) is the first official update and has been widely anticipated. Although compliance with the NIST framework is generally voluntary, U.S. Government agencies have mandated adoption of NIST-Framework-based cybersecurity policies in particular contexts, including Team Telecom mitigation instruments and government contracts.

## 1. What's new (and what the changes really mean)

As the name "Version 1.1" suggests, the updated Framework is an incremental update that refines, clarifies, and enhances Version 1.0 while retaining many of its core features. Overall, NIST aimed to make these changes compatible with Version 1.0. That said, the updated Framework contains several key updates that companies should review in shaping their cybersecurity strategies. Among other things, Version 1.1:

- *Expands the applicability of the Framework, while retaining its voluntary nature*.

Although NIST originally intended Version 1.0 to apply only to organizations with a nexus to U.S. critical infrastructure, organizations of all stripes have used the Framework as a roadmap for conducting a cybersecurity risk assessment. Indeed, the Framework has been translated into a wide variety of languages, and it continues to be a focus of international standards bodies. Version 1.1 recognizes that reality, noting that the Framework is useful for addressing cybersecurity for any organization relying on technology, regardless of whether it operates critical infrastructure and regardless of whether it operates in the U.S. With this change, organizations that have not conducted a risk assessment that is consistent with the NIST Framework could face increasing market-based pressures to do so.

Government pressure on organizations to adopt the Framework is also a possibility. Version 1.1 made clear that use of the Framework continued to be voluntary. However, governments outside of the U.S. could adopt a modified version of the Framework that is mandatory or highly encouraged. And while U.S. government agencies are unlikely to require adoption of the NIST Framework by regulation, some agencies impose a de facto or contractual requirement in bilateral contexts. One example is a transaction where a foreign investor seeks to gain an interest in a U.S. company, and the transaction is subject to review by the Committee on Foreign Investment in the United States. A key consideration for the CFIUS in evaluating a transaction's potential impact on U.S. national security (and thus whether the CFIUS will allow the transaction to be consummated) is an assessment of the company's cybersecurity risk profile and whether data vulnerabilities exist – particularly with respect to critical technology, critical infrastructure, and the collection and storage of large amounts of personally identifiable information. Demonstrating how a company has identified and mitigated risks by using the

Version 1.1 Framework may be a helpful way for a company to demonstrate sound cybersecurity risk management practices in a way familiar to the CFIUS.

- *Confirms that "compliance with the Framework" is not a useful criterion.*

The Framework was never designed to be a checklist of cybersecurity action items for all organizations. Instead, Version 1.0 recognized that organizations have "different threats, different vulnerabilities, different risk tolerances" and will respond to those factors in various ways – all of which are consistent with the Framework. However, under Version 1.0, key players frequently spoke about "compliance with the Framework" in business and cybersecurity settings, which obscured underlying differences in what the key players actually meant.

Version 1.1 makes explicit that "compliance with the Framework" is not a useful concept and does not have a commonly accepted meaning. As a result, organizations have new ammunition for seeking details from vendors and other organizations on their cybersecurity practices, beyond pat assertions of Framework compliance. Additionally, organizations that have viewed "compliance with the Framework" as a panacea should reevaluate their approaches.

- *Encourages quantitative and business-focused analysis of cybersecurity.*

One of the larger changes in Version 1.1 is a new section on "*Self-Assessing Cybersecurity Risk with the Framework*." This new section addresses how organizations might, during the course of their risk assessment, "measure and assign values to their risk along with the cost and benefits of steps taken to reduce risk to acceptable levels."

NIST's original proposals on this topic resulted in widespread debate and criticism from industry, including a number of very vocal critics in the telecommunications sector. NIST's original, draft title of this section was "Measuring and Demonstrating Cybersecurity," which many in industry read to imply that organizations would be required to measure and demonstrate cybersecurity using one-size-fits-all metrics. NIST indicated that its final title should signal a shift toward an organizational-specific, rather than prescriptive, approach. Moreover, in a recent webcast, a NIST presenter made clear that while additional materials regarding this section might be forthcoming, those materials would be focused on "defining the relationship between cybersecurity outcomes and business objectives," rather than on measurement of compliance with the Framework alone.

Measuring the effectiveness of a cybersecurity program, with an eye toward a holistic understanding and program for improving risk management, can serve many laudable business goals. But measuring the effectiveness of a cybersecurity program at risk presents potential pitfalls that companies should consider as they implement Version 1.1.

**Consider context**: Companies should avoid applying generic measurements for the sake of merely collecting data on cybersecurity practices without looking to the unique circumstances of an organization's specific profile, goals, and desired outcomes.

**Avoid Self-Imposed Standards:** Companies should be wary of assigning "grades," quantitative comparisons among divisions or to peer organizations, or time-based "progress reports" with respect to cybersecurity risk management. These and similar rating exercises can contribute to a *de facto* standard of care that the company may be legally expected to meet.

**Measurements Today, Liability Tomorrow?:** Although a company's internal assessment of its own cybersecurity risk profile and potential gaps can help improve the IT infrastructure, if not properly designed, such an exercise can potentially lead to greater exposure in the event of cybersecurity incident litigation. Companies should consider appropriately integrating counsel into a cybersecurity risk assessment (or incident response), for the purpose of the appropriate consideration of regulatory and legal factors and for privilege purposes.

- *Cyber Supply Chain Risk Management.*

Version 1.1 greatly expands on its discussion of Cyber Supply Chain Risk Management (CSCRM), highlighting, among other things, risks associated with commercial off-the-shelf products and services. Responding to input from the business community, the Version 1.1 takes an educational and awareness-raising tone. It focuses on how organizations with their own cybersecurity requirements can effectively convey those requirements to partners, suppliers, and other stakeholders – and ensure that stakeholders follow through. It also provides a prioritized list of cybersecurity measures that organizations can use as a reference when choosing vendors.

**2. What to watch out for going forward**

Version 1.1 is designed to be flexible—so each organization's response will be different. At a high level, companies in the telecommunications sector should keep an eye on how the Communications Security, Reliability and Interoperability Council responds to the update. Global companies with cross-border concerns should keep an eye on the degree to which the Framework continues to be voluntary in nature for all relevant jurisdictions. Organizations looking to engage directly with NIST may wish to attend NIST's Cybersecurity Risk Management Conference, scheduled for November 6-8 in Baltimore, Maryland, where the Framework is expected to be a major focus. And companies looking to reassess their cybersecurity regulatory advocacy or compliance strategies should consult with counsel for advice specific to their circumstances.

* * * *

For more information on the impact of changes in NIST's updated Cybersecurity Framework, please contact Kent Bressie, Adrienne Fowler, Robert Friedman, Michael Carlson or the HWG lawyer with whom you regularly work.

*This advisory is not intended to convey legal advice. It is circulated as a convenience and is not intended to reflect or create an attorney-client relationship as to its subject matter.*