February 23, 2016

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, M.D. 20899

Re: Response to Request for Information (RFI) regarding the Framework for Improving Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

The National Restaurant Association ("NRA") is the leading business association for the restaurant and foodservice industry, which is comprised of nearly one million locations employing 14 million people who serve 130 million guests daily.

Data security is an ongoing and growing concern for restaurants across the country. Innovations in technology have only just begun to help our members streamline their operations, reduce their costs and bring more guests into their restaurants. These innovations – whether in payments, marketing, operations and beyond – often depend on large amounts of valuable data that hackers so desperately want. The Framework for Improving Critical Infrastructure Cybersecurity ("Framework") offers our members a broad but accessible risk-based approach to protecting restaurants and their customers' data.

For the past several months, NRA has engaged in multiple efforts to promote awareness and use of the Framework by our members. NRA produced and released a guide, "5 Essential Steps for an Enterprise-wide Cybersecurity Program," to educate our members on how to secure their operation through a focus on the Core of the NIST Framework – Identify, Protect, Detect, Respond and Recover. These five functions, which are broken down into categories and subcategories and then cross-mapped to up-to-date applicable standards and best practices, provide the most useful and actionable information for our members. NRA has also convened a working group of member company representatives to formulate a Cybersecurity Framework for the Restaurant Industry, a sector-specific cybersecurity guidance based on the Framework for use by single-unit restaurant operators. More than seven in ten restaurants are single-unit operations. Lastly, we have promoted the Framework through webinars with NIST and hosting NIST at industry events.

In response to the RFI, we offer the following observations based both NRA's direct experience with the Framework as well as feedback from our members.

First, the RFI specifically asks if the Framework should be updated. NRA believes no updates or changes may be necessary at this time. The Framework was designed to be flexible and adaptable according to need and segment. The restaurant industry can use the same Framework as the basis for their specific industry guidance as did the telecommunications industry, water sector and many other organizations. These different uses are emblematic of its truly versatile nature.

If changes were to be considered, then NRA and our members offer the following suggestions. First, use of the term "critical infrastructure" in the Framework's official title – "Framework for Improving the Cybersecurity of Critical Infrastructure" – may be a deterrent to those who are not aware of the various components of "Critical Infrastructure." It may be best to rename the Framework without this reference in order to encourage the more widespread adoption and ongoing use of it by organizations large and small, involved in critical infrastructure or not.

Second, despite the broad and accessible approach that we highlighted above, the terminology used in the Framework and supporting documents may still be too complicated and difficult to understand by a small or medium sized business owner, and therefore may limit the widespread use of the Framework. As noted above, NRA, like other trade associations to date, has convened a group to translate and prioritize the larger Framework into useful tool for single-unit restaurant operators. Nevertheless, we recognize that other market segments may not have the resources to convene and support such an effort. To overcome this limitation, NIST and/or other agencies, such as the U.S. Small Business Administration, the U.S. Computer Emergency Readiness Team, Federal Trade Commission and/or the U.S. Department of Homeland Security, should coordinate and/or align their efforts to create a unified version of the Framework and supporting materials for general use by small and medium sized businesses. It is clear from the wide industry acclaim and support for the Framework that it is the trend in cybersecurity planning. Therefore, the use of it should be enabled and promoted by other federal agencies.

Third, NIST should consider including Payment Card Industry Data Security Standards (PCI-DSS) in the Framework's references to cybersecurity standards, guidelines, and practices where appropriate considering that PCI-DSS generally applies only to the protection of payment card information. The merchant community must comply with PCI-DSS if they chose to accept credit cards. By incorporating PCI-DSS into the Framework, NIST may ease adoption by small and medium sized merchants.

Fourth, the RFI asks how the Framework could prevent duplication of regulatory requirements. Some have suggested mandatory Framework adoption in lieu of duplicative requirements. This approach ignores the Framework's most laudable attribute, as noted above: its flexibility. To make the Framework a regulatory requirement would shift resources and attention away from security and risk management towards compliance. Static compliance activities, while important, are no substitute for risk-based management of quickly-changing cybersecurity threats, which is the intention of the Framework.

Finally, NRA and its members have found resources included under "Industry Resources" on the Framework's webpage to be the most useful as we consider the form and content of Cybersecurity Framework for the Restaurant Industry. We have also been grateful for the direct interaction between our members and NIST staff during webinars and industry events we have hosted.

We look forward to continuing to promote the Framework and work with NIST on this critically important issue.

Sincerely,

Laura Knapp Chadwick
Director, Commerce & Entrepreneurship
National Restaurant Association