Before the Department of Commerce
Washington, D.C.

In the Matter of	**)**	
	)	
Guide to Cyber Threat Information	**)**	**NIST Special Publication 800-**
Sharing (Draft)	**)**	**150 (Draft)**
	)	

COMMENTS OF CTIA – The Wireless Association

Submitted: November 28, 2014

CTIA – The Wireless Association
Expanding the Wireless Frontier
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-0081
www.ctia.org

Michael F. Altschul
Senior Vice President, General Counsel

John M. Marinho
Vice President, Technology and
Cybersecurity

Table of Contents

I. Introduction **1**

II. The limited scope and nature of SP 800-150 should be clear. **1**

A. The Guide should clarify its application to federal systems and agencies. 1

B. NIST should not promote particular substantive measures or policy outcomes. 2

C. Cyber information sharing should be defined precisely and consistently. 3

III. Despite obstacles, diverse information sharing is occurring and should be encouraged, including with legislation. **4**

A. Varied legal regimes can apply to sharing in different settings. 4

B. NIST should encourage the use of varied models and venues, rather than promoting one approach to information sharing. 5

IV. Conclusion **6**

I. INTRODUCTION

CTIA members appreciate the cybersecurity efforts of the National Institute of Standards and Technology ("NIST"), including the *Framework for Improving Critical Infrastructure Cybersecurity* ("*Framework*")[1] and NIST's Special Publication 800-150, *Guide to Cyber Threat Information Sharing (Draft)* ("*Guide*" or "SP 800-150").[2] On behalf of our members, CTIA welcomes the opportunity to comment on the draft *Guide*.

On all cybersecurity matters, CTIA supports a non-regulatory approach that will provide flexibility to use the most effective tools to combat evolving threats. CTIA's view of information sharing is no different; we laud its benefits and urge improvements to increase flexibility, as explained in a recent whitepaper.[3]

NIST has a long history of using a non-regulatory, voluntary, and collaborative approach to technical and operational challenges. On cybersecurity, NIST has been an effective convener of the private sector and government to address the security of federal systems. NIST is continuing this role in helping federal entities share information; SP 800-150 can promote information sharing and help government agencies identify areas for attention, in particular by reinforcing the common language put forward in the *Framework*. While the *Framework* process is ongoing, however, NIST should ensure that SP 800-150 is focused on federal government users and does not promote substantive standards or information sharing methods.

CTIA offers some suggestions to clarify the draft. NIST should make clear that SP 800-150 is focused on the federal government. Given the impact NIST can have on public and private actors, NIST should ensure that its focus remains on information sharing—not promoting particular substantive cyber risk management practices. In addition, a great deal of experimentation is happening on cyber, and sharing takes many forms. CTIA urges NIST to validate the significant barriers that impede information sharing. Finally, while policy makers debate solutions, NIST should encourage varied approaches and avoid steering entities to one model for sharing.

II. THE LIMITED SCOPE AND NATURE OF SP 800-150 SHOULD BE CLEAR.

A. The Guide should clarify its application to federal systems and agencies.

In keeping with NIST's non-regulatory, voluntary, and collaborative approach to cybersecurity issues, NIST should consider clarifying that the *Guide*'s intended audience is federal systems and agencies, not the private sector. The draft explains that "NIST is responsible

---

[1] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0 (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
[2] NIST, *Guide to Cyber Threat Information Sharing (Draft)* (Oct. 2014), *available at* http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf ("*Guide*").
[3] CTIA, *Today's Mobile Cybersecurity Information Sharing*, 3 (Sept. 9, 2014), *available at* http://www.ctia.org/docs/default-source/default-document-library/ctia_informationsharing.pdf ("*CTIA Information Sharing White Paper*") ("[Cybersecurity information sharing] serves as the essential and critical shield in the ongoing struggle to protect mobile devices, laptops and wireless Internet-based services against cyberthreats.").

for developing information security standards and guidelines, including minimum requirements for federal information systems,"[4] and that "[t]his guideline has been prepared for use by federal agencies."[5]

The final *Guide* could be clearer in identifying its audience and scope, which is for use by government agencies to protect government systems. In some respects, the draft *Guide* seems to address issues, capabilities, and scenarios beyond government systems. In Appendix A, NIST reviews seven incident coordination scenarios, but only two of those scenarios involve a government-based sharing arrangement.[6] NIST can easily clarify the intended audience for SP 800-150 throughout the document. For example, NIST should consider clarifying the title, which could read: *Guide to Cyber Threat Information Sharing for Federal Systems*.

B. NIST should not promote particular substantive measures or policy outcomes.

The *Guide* can be a valuable tool to streamline and promote information sharing. It should not appear to endorse specific cybersecurity measures, require use of NIST's voluntary *Framework*, or encourage particular policy outcomes.

SP 800-150 could be clarified by addressing instances where NIST seems to tread outside of guidance related specifically to cyber information sharing. NIST's document is premised on the notion that information sharing will rely on and build a mature cyber capability, from detection and defensive capabilities,[7] to incident response plans.[8] Among other things, NIST urges "routine self-assessments to identify opportunities for improved cybersecurity practices,"[9] and it discusses at length core and advanced cybersecurity capabilities. NIST supplies recommendations and expectations, for example, with respect to internal information handling.[10] NIST envisions improved substantive cyber capabilities being leveraged in a virtuous cycle of sharing in which indicators, capabilities, and responses are all accessible, shared, and refined for maximum benefit. These recommendations wade into substantive cyber preparedness and response, which is particularly troubling if NIST does not clarify that this document is not intended to apply beyond a narrow government audience.

---

[4] *Guide*, at ii, 4.
[5] *Id.* at 4.
[6] *Id.* at 56–58. Scenario 3 involves an Information Sharing and Analysis Center ("ISAC"), *id.* at 56–57, and Scenario 6 involves the United States Computer Emergency Readiness Team ("US-CERT"), *id.* at 58. Other scenarios involve private systems and private sector sharing.
[7] *See e.g.*, *id.* at 2–3 (recommending enhanced "local data collection and analysis capabilities," and urging that "[o]rganizations should engage the adversary throughout the cyber attack life cycle and develop and deploy defensive measures").
[8] *See, e.g.*, *id.* at 64–67 (listing resources for incident response capability).
[9] *Id.* at 26.
[10] NIST encourages organizations to take various internal steps in evaluating and handling data, and in structuring operations. For example, NIST suggests inventorying "information that supports key business functions (*e.g.*, financial, employee, or customer data that may contain PII [Personally Identifiable Information]; intellectual property). *Id.* at 28. And NIST observes that "[a]n organization may benefit from integrating security and privacy incident and breach response processes, as the processes are mutually supportive." *Id.* at 32.

NIST should be cautious not to use the *Guide* to promote or require adoption of the voluntary *Framework* or portions thereof. In the current draft, recommendations from the *Framework* are central to NIST's specific information-sharing vision.[11] However, because the *Framework* is new, sectors are still evaluating whether and how it can be useful. Particularly because the *Framework* was intended to be voluntary, it would be premature to import into government information sharing guidance any substantive solutions from the *Framework*.

C. Cyber information sharing should be defined precisely and consistently.

Cyber information sharing is complex and situation-dependent. Because of this, it is critical to have a clear, common understanding of what information sharing means. Too often, policy discussions are based on imprecise terms. NIST should consider defining the task at hand and sticking closely to that definition throughout the *Guide*.

NIST could more precisely and consistently define "cyber threat information." The current draft *Guide* defines the term in Appendix B as "[i]nformation (e.g., indications, tactics, techniques, procedures, behaviors, motives, adversaries, targets, vulnerabilities, courses of action, or warnings) regarding an adversary, their intentions, or actions against information technology or operational technology systems."[12] But throughout the document, NIST does not often use that term of art, instead discussing collaboration and the sharing of information and intelligence generally. NIST could consider a more precise definition, with reference to the type of information to be shared and the circumstances under which the information is to be shared. NIST should refer to such a definition more often throughout the document.

In CTIA's view, "cybersecurity information sharing" is:

> the sharing of information in a *confidential, trusted setting, which means a protected legal and legislative environment, exclusively for cybersecurity purposes*. Cybersecurity purposes include: indicators of cyberthreats and attacks; monitoring of threats and application of countermeasures; and discussions and findings about development and testing of new defenses and standards, with the aim of preserving and strengthening security across communications networks and systems.[13]

CTIA has developed examples of what cyber information sharing is—and is not. For example, cyber information sharing *is* "[a]ccomplished only when all parties are protected from liability, including antitrust and litigation concerns," but *is not* "[d]iscussion or collaboration on pricing, markets or any other matter that is viewed as competitive under antitrust law."[14] NIST should consider such definitions and examples to the extent that they are useful.

---

[11] *Id.* at 19 ("An organization should move from informal, ad hoc, reactive cybersecurity approaches where the organization operates in isolation to formal, repeatable, adaptive, proactive, risk-informed practices where the organization coordinates and collaborates with partners; such an approach is described in the Cybersecurity Framework.").
[12] *Id.* at 59.
[13] *CTIA Information Sharing White Paper*, at 5 (emphasis in original).
[14] *Id.*

III. DESPITE OBSTACLES, DIVERSE INFORMATION SHARING IS OCCURRING AND SHOULD BE ENCOURAGED, INCLUDING WITH LEGISLATION.

A. Varied legal regimes can apply to sharing in different settings.

Significant barriers to information sharing limit a more robust response to cyber threats. A variety of legal obligations apply to information sharing in different settings, from federal criminal law, to antitrust concerns, to the risk of Freedom of Information Act ("FOIA") disclosures.[15] Classification rules can constrain dissemination of information from the government. International obligations add complications. And, cyber and data security are an increasing focus of federal regulators like the Federal Trade Commission and Federal Communications Commission, who promise vigorous oversight of how systems and consumers' personal information are secured.[16] This fluid landscape chills more effective information sharing, both directly with the government, and within coordinating councils in which the government participates.

NIST notes that challenges accompany information sharing, but it could more plainly acknowledge the significance of existing barriers and their impact. NIST refers to "restrictions" that may be imposed by an organization's "executive and legal team," but in doing so, distinguishes between "legitimate" concerns and "unwarranted or arbitrary" restrictions.[17] This implies that some concerns are not well-founded. In its description of "Challenges to Coordination and Sharing," for example, NIST recognizes the threat of disclosure, and simply urges organizations to "manage these risks using an appropriate risk management strategy."[18]

The *Guide*'s discussion about "information sensitivity" recognizes that an organization must consider multiple variables to determine when it can share information, but ultimately advises that "[t]he information owner, management, and legal teams should adjudicate all sharing decisions using established procedures."[19] Similarly, with respect to personally identifiable information ("PII"), NIST notes that organizations manage privacy risks with legal, policy and technical personnel. NIST broadly observes without clarification that "threat

---

[15] *Id.* at 16–20 (highlighting information sharing limitations, including the lack of clarity regarding whether carriers can immediately share information about botnet attacks with other carriers and/or affected customers).

[16] *See, e.g.*, Jessica Rich, Director, Bureau of Consumer Protection, FTC Testimony before the Senate Committee on Banking, Housing and Urban Affairs, Subcommittee on National Security & Int'l Trade & Finance (Feb. 3, 2014) (noting FTC's record of "50 cases against businesses that it charged with failing to provide reasonable protections for consumers' personal information) available at http://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-safeguarding-consumers-financial-data/140203financialdatasecurity.pdf); *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (upholding FTC action against a company for failing to maintain adequate data security for sensitive personal information); *see also TerraCom, Inc. & YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, FCC 14-173 (Oct. 24, 2014) (proposing a $10 million fine against companies that allegedly failed to protect sensitive personal information, "expos[ing] their customers to an unacceptable risk of identity theft and other serious consumer harms).

[17] *Guide*, at 8.

[18] *Id.*

[19] *Id.* at 32–33.

information that is shared externally is focused on actionable information for other organizations and should not contain PII."[20] Whether this is normative or positive is unclear, but given ongoing policy discussions,[21] NIST should avoid weighing in on the proper extent of protections related to PII in various cyber information sharing settings.

CTIA urges NIST to acknowledge that substantial legal uncertainties and risks exist, for example from lawsuits, public criticism, and other dangers associated with sharing various types of information in different settings. NIST should confirm that these risks are barriers to more effective information sharing. As CTIA has long advocated, these obstacles require legislative action,[22] which would guide and foster more robust sharing partnerships, and therefore, more effective answers to cyber threats.

B. NIST should encourage the use of varied models and venues, rather than promoting one approach to information sharing.

Despite these significant barriers, robust and effective cyber information sharing is occurring.[23] Within the wireless industry, for example, CTIA's members have cultivated a variety of information-sharing organizations and relationships, which fit both the hub-and-spoke and the peer-to-peer models identified by NIST. Based on hard work and collaboration, "a wide array of public-private forums [have formed] over time as a result of threats . . . to the integrity of U.S. infrastructure, including its communications networks and systems."[24] Today, organizations throughout the ecosystem—communications companies, software developers, providers, third party vendors and consultants—share information. They interact with diverse government bodies, with each other, and with customers—both end users and those in the supply chain—in diverse settings and subject to varied regimes, including different levels of contractual obligation. These information-sharing activities can be formal or informal, depending on the circumstances.

---

[20] *Id.* at 30.

[21] *See, e.g.*, *Guide*, at 30 n.17 (discussing varied definitions of PII); Statement by the President on the Cybersecurity Framework, The White House Office of the Press Secretary (Feb. 12, 2014), *available at* http://www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework ("I again urge Congress to move forward on cybersecurity legislation that both protects our nation and our privacy and civil liberties.").

[22] *See CTIA Information Sharing White Paper*, at 16 ("Legislation is needed to provide legal certainty, and thereby enable a more real-time, active cybersecurity threat response capability."); *see also* Letter from CTIA, et al. to Rep. Mike Rogers, Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence and Rep. C.A. Ruppersberger, Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence (Dec. 15, 2011), *available at* http://blog.ctia.org/2011/12/15/ctia-and-ceos-from-8-providers-support-cyber-intelligence-sharing-and-protection-act-of-2011/ (urging the adoption of legislation "to facilitate appropriate sharing of cyber-defense information between the federal government and the private sector, as well as among private sector entities").

[23] *CTIA Information Sharing White Paper*, at 9 (describing that "advances in structured cybersecurity information sharing over the past decade . . . are evident in the relatively low rates of malware encounters in [the United States] as compared with much of the rest of the world").

[24] *Id.* at 4 (noting that members "actively participate in . . . industry and government partnerships").

NIST should recognize the existing diversity of approaches and encourage varied information sharing, all of which can benefit government agencies and systems. NIST should not endorse hub-and-spoke models versus peer-to-peer models, nor should it endorse formal models versus informal models. Valuable collaboration occurs in formal structures, public-private partnerships, ad hoc cooperation, vendor relationships, work with third party researchers, and innovative managed service arrangements. Standards are evolving to govern sharing in diverse settings, including the development of common languages and methods for describing vulnerabilities, as well as challenges surrounding data classification and the aging of threat intelligence. These issues are complex and changing, as participants refine their practices.

Elevating one form of information flow, or promoting a particular degree of formality, could create an incentive toward that, at the expense of other effective solutions. Preferring one approach may overlook some of the innovations underway, which can benefit federal agency customers and systems as well as private. A premature preference for particular methods or venues may discourage the flexibility necessary to face evolving cyber threats. NIST should make clear that all options should be available and—particularly while cyber information sharing is evolving and barriers remain—there is no one "right" solution.

IV. CONCLUSION

CTIA appreciates NIST's work as a convener bringing industry and government together to address cyber threats and share practices, solutions, and perspectives. Information sharing is key to effective cybersecurity. CTIA has urged Congress to pass legislation to streamline the sharing of cybersecurity information, helping us anticipate and respond to the challenges ahead. In the meantime, efforts to describe and improve information sharing should continue, focusing on raising awareness and expertise, while avoiding prescriptive approaches that wade into substantive policy choices. NIST should continue to foster the collaborative, non-regulatory approach that worked so well and promises to help refine solutions to secure federal and other systems in the future.