**Cyber Threat Alliance, Inc.**
1001 19th Street North, Suite 1200
Arlington, Virginia 22209

The Cyber Threat Alliance (CTA) appreciates the opportunity to provide feedback on the Cybersecurity Framework Draft Version 1.1. CTA currently encompasses 14member companies, including Checkpoint, Cisco, Eleven Paths, Fortinet, IntSights, McAfee, Palo Alto Networks, Rapid 7, RSA, Reversing Labs, Saint Security, SK Infosec, Sophos, and Symantec.

CTA strongly supports the Framework as a tool for managing cyber risk. It has become a valuable reference document not just within the U.S., but globally, and we believe it is very important to continue to build on the original quality product. Overall, we support the edits and updates proposed for the framework. We would offer the following specific comments:

1) Information and intelligence sharing forms a key element of the Framework in two ways. One is in the Framework Tiers. Generally, the higher the tier, the more information sharing an organization is supposed to do. The other is in the Framework core, in the Identify functional area (ID.RA-2: "Cyber threat intelligence is received from information sharing forums and sources") and in the Respond functional area (RS.CO-5: "Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness" and RS.AN-5: "Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources [e.g., internal testing, security bulletins, or security researchers]").

   Comment: CTA strongly supports the Framework incorporating intelligence and information sharing in these two contexts. However, the Framework should make clear, most likely in the Executive Summary or Framework Introduction, that effective information sharing does not just mean sharing technical indicators, but also encompasses sharing information about threat context, business operations, best practices, threat awareness, vulnerabilities, etc. For the Framework tiers, the Framework should state that the kind of information sharing an organization gets involved in should reflect its overall business operations and that not every organization needs to be sharing or trying to consume technical indicators. Finally, the Framework should emphasize that the purpose of sharing information is to influence actions and change behavior, improving an organization's cybersecurity regardless of how its enterprise is configured. Whenever possible and reasonable, organizations should look for opportunities to encourage their cybersecurity providers to enable automated ingestion of indicators to speed up cybersecurity, or if they are able to consume technical indicators themselves, seek such automation internally.

**Cyber Threat Alliance, Inc.**
1001 19th Street North, Suite 1200
Arlington, Virginia 22209

Reason: Most organizations have difficulty producing or consuming technical indicators for themselves (large banks are the exception, not the rule). Instead of trying to get every organization to produce or consume technical cybersecurity information, certain key players in the ecosystem need to be the focus of the technical indicator sharing, such as cybersecurity companies, telecommunications companies, and large IT service providers. Other organizations need to focus on sharing intelligence and information directly relevant to their business operations and that helps the company make risk-informed cybersecurity decisions.

2) Section 3.6 on the Methodology to protect privacy and civil liberties has improved, but the focus remains exclusively on the threat that cybersecurity practices could pose to privacy.

   Comment: While true that poor cybersecurity practices could pose a privacy risk, the Framework should also discuss how cybersecurity and privacy are mutually reinforcing. For example, this section could include language along these lines:

   "In the digital age, good cybersecurity practices will protect the personal information of organization's clients, customers, and employees from malicious actors. However, good privacy policies also improve cybersecurity. Effective privacy policies drive an organization to think about the data it has, why it has it, and whether it needs to keep the data and for how long, and how it wants to protect it. Additionally, organizations should identify ways to enforce and automate privacy risk mitigation policies at speed and scale, just as they strive to do with cybersecurity. In this manner, organizations can improve cybersecurity and privacy in tandem. Conducting this analysis is a critical element of the Identify functional area in the Framework Core."

   Reason: The more significant threat to privacy comes from malicious cyber actors rather than the cybersecurity policies in most organizations. Also, as noted, good privacy policies force a needed conversation in an organization. The Framework should reflect these aspects of the privacy and cybersecurity relationship. Further, good privacy policies facilitate rapid information and intelligence sharing, because companies then have a clear idea of what information can be shared, with whom, and under what conditions.

3) The revised Framework has a section on self-assessment (Section 4). This section urges organizations to conduct self-assessments and measure their progress in reaching the target states.

**Cyber Threat Alliance, Inc.**
1001 19th Street North, Suite 1200
Arlington, Virginia 22209

Comment: CTA strongly supports the development and use of effective cybersecurity performance metrics in self-assessments. However, as drafted, this section suffers from some weaknesses:

A. This section's purpose is not clear. If the Framework is only going to urge companies to conduct self-assessments, then it could promote that concept with fewer words. On the other hand, if we want the Framework to help companies think about self-assessments, then this section needs to be more robust.
    a. If the former, then the section should be scaled back.
    b. If the latter, the Framework should include pointers to the best known work on cyber assessments.
B. The section does not acknowledge how weak cybersecurity performance metrics are right now and the challenges most organizations will face in selecting the right measurements.
C. The section should acknowledge that judging cyber risk is difficult activity that will require practice and needs to be periodically re-visited. It is not a "one and done" activity for an organization.
D. The section discusses leading and lagging measurements, but does not define those terms nor give examples.
E. This section should call on the private sector to continue developing self-assessment tools, methodologies, and performance metrics.

Reason: Self-assessments are a key tool for organizations to use in managing their cyber risk. However, this field remains under-developed, and most organizations would be challenged to conduct an effective self-assessment. If intended to help organizations think through how to conduct self-assessments, this section needs to point toward some additional resources.

4) Supply chain risk management is a new area in the Framework.

Comment: CTA concurs that supply chain risk represents a significant cyber threat and that incorporating it into the Framework makes sense.

Reason: Overall, the language here is useful, and it fills in a gap in the original Framework.

Sincerely,

J. Michael Daniel
President & CEO
Cyber Threat Alliance