DORSEY
DORSEY+WHITNEY LLP

Release of National Cyber Strategy

September 25, 2018 – The TMCA
by Cody Wamsley

Late last week, the Trump Administration released the National Cyber Strategy of the United States of America, purportedly the first such document released by the government in 15 years. According to the introduction by the President, the Cyber Strategy "is a call to action for all Americans **and our great companies** to take the necessary steps to enhance our national cybersecurity" (emphasis added). The new Cyber Strategy outlines four pillars for advancing the cybersecurity posture of the United States:

1. Protect the American People, the Homeland, and the American Way of Life
2. Promote American Prosperity
3. Preserve Peace through Strength
4. Advance American Influence

Language in the first pillar indicates a significant effort may be forthcoming by the federal government to improve threat intelligence sharing with the private sector:

- The United States Government will strengthen efforts to share information with ICT [Information and communications technology] providers to enable them to respond to and remediate known malicious cyber activity at the network level. This will include sharing classified threat and vulnerability information with cleared ICT operators and downgrading information to the unclassified level as much as possible.

In the same section, the Cyber Strategy indicates a heightened focus on third party information security risk:

- We will promote an adaptable, sustainable, and secure technology **supply chain that supports security based on best practices and standards**. The United States Government will convene stakeholders to devise cross-sector solutions to challenges at the network, device, and gateway layers, and we will encourage **industry-driven certification regimes** that ensure solutions can adapt in a rapidly evolving market

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

and threat landscape.

Finally, the language contained in the third pillar, coupled with statements last week by National Security Adviser, John Bolton, have been generating quite a buzz in the cybersecurity community as they signal a shift of American posture in the cyberwarfare arena to a strategically offensive posture. Of note in the third pillar is this language:

- "**All instruments of national power** are available to prevent, **respond to**, and **deter** malicious cyber activity against the United States. This includes diplomatic, information, **military** (both kinetic and **cyber**), financial, intelligence, public attribution, and law enforcement capabilities. The United States will formalize and make routine how we work with like-minded partners to attribute and deter malicious cyber activities with integrated strategies that **impose swift, costly, and transparent consequences** when malicious actors harm the United States or our partners."
- "The United States will work with partners when appropriate to impose consequences against malicious cyber actors in response to their activities against our nation and interests."
- "The United States will use all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation. This includes working with foreign government partners **as well as the private sector**, academia, and civil society to identify, **counter**, and prevent the use of digital platforms for malign foreign influence operations while respecting civil rights and liberties."

(emphases added)

In all, it is yet to be seen what mandates may stem from this strategy to the private sector, but it stands to reason that the current administration will be heightening its focus on private sector cooperation in defending the nation's infrastructure. Companies, particularly in the IT sector, should recognize that a new focus on threat intelligence sharing, vendor management, and even the possibility of participating in offensive capabilities are on the near horizon and should begin evaluating their current posture on these fronts (and others mentioned in the Cyber Strategy).