# Trump Administration Signals Greater Private Role in Offensive Cyber Operations

MARCH 9, 2026

On Friday, March 6, the Trump Administration released its national cyber strategy. In this client alert, we evaluate what the final strategy means for defense contractors supporting government offensive cyber operations, as well as for companies looking to defend their own assets and other privately held critical infrastructure from cyberattacks.

As previewed by administration officials over the past few months, the final strategy includes six pillars: 1) Shape Adversary Behavior; 2) Promote Common Sense Regulation; 3) Modernize and Secure Federal Government Networks; 4) Secure Critical Infrastructure; 5) Sustain Superiority in Critical and Emerging Technologies; and 6) Build Talent and Capacity. Leading up to its release, there was significant speculation surrounding the strategy's approach to offensive cyber operations, including reporting suggesting it might pave the way for more private sector participation in offensive cyber operations or even companies being authorized to "hack back."

Notably, the strategy contemplates a greater role for private industry in working with government on cyber-related matters. According to the strategy, the administration "will unleash the private sector by creating incentives to identify and disrupt adversary networks and scale our national capabilities." In parallel, the administration pledges to "use all instruments of national power" against nation-state and criminal actors. The administration frames private sector contributions as part of this "collective effort" to defend cyberspace from a range of adversaries.

While the strategy offers limited specifics, it broadly underscores a more assertive outlook toward cyber deterrence. The government's efforts will likely flow from an infusion of resources, such as the $1 billion appropriation for offensive cyber operations in the One Big Beautiful Bill Act, and a recent Executive Order addressing cybercrime. As government investment in cyber deterrence increases, we anticipate that private sector opportunities will mean expanded government contracts and law enforcement partnerships. Those opportunities can bring real gains for companies and for US national security—but they also carry with them material risks that merit careful consideration and mitigation, as we explain below.

**The strategy foreshadows more opportunities for defense contractors for involvement in offensive cyber operations.**

The strategy signals an overall greater reliance on offensive cyber operations to prevent cyberattacks. According to the strategy, the administration's goal is to "detect, confront, and defeat cyber adversaries before they breach [US] networks and systems."

Offensive cyber operations can encompass a broad range of activities and include, perhaps counterintuitively, actions that are primarily defensive in purpose. The Department of Defense generally considers offensive cyber operations to be any operations conducted outside of those networks protected by the government and its partners, regardless of whether there are intended kinetic effects. The myriad of laws, including anti-hacking statutes, generally limiting these actions to the government's purview has not changed. However, the strategy may portend transformative changes in the government contracting space to address capacity limitations on the part of the government in keeping up with adversarial activity in the cyber domain.

The actual scope of this transformation, including the key question of what role the US government envisions for the private sector in supporting and carrying out offensive cyber operations at the direction of the government, could vary. In-house counsel advising on potential business opportunities should watch for follow-on guidance and implementation trends in two key areas.

### A. "Inherently Governmental" Limitations in Cyber Operations

Historically, defense contractors have generally supported the military and intelligence community in "defensive" cyber operations, though this line has grown fuzzy over time as more operations expand into "preparing the battlespace" within adversary networks. While defense contractors operate under federal authorities, including Title 10 and Title 30, agencies have adopted cautious legal interpretations of "inherently governmental activities" that sharply constrain contractor roles in operations with potential real-world effects or unintended harm to third parties.

The new cyber strategy sets a forward-leaning policy that could invite reexamination of those limitations. Government lawyers, in particular, may understand the strategy to present an opportunity to update legal interpretations to reflect the technological and operational landscape. Opening the aperture for greater private-sector involvement would, in turn, serve the strategy's goal of increasing overall cyber capacity in service of US government objectives.

Whatever alterations might be made, companies seeking to work with the government should obtain explicit instructions for all aspects of offensive cyber activities to establish that they are operating at governmental direction and control at every step. This is a key element of government contractor defenses to conceivable future claims and is, moreover, important to establish the protection of derivative immunity when operating on behalf of the government.

### B. The Application of Federal Acquisition Regulation Indemnification Rules to High-Risk Cyber Activities

Both legacy defense contractors and less traditional defense tech companies are likely to see opportunities for bigger roles in cyber operations as the new strategy is implemented. At the same time, they will need to mitigate risks in an area of substantial uncertainty. There are a range of state

laws and common law doctrines that could expose contractors to liability for harm caused to innocent third parties in the context of fulfilling high-risk cyber requests made by the government. These parties may pursue compensation through property damage, negligence, trespass, or breach of contract claims, among others arising under tort law. For especially high-risk activities—where losses are potentially uninsurable—contractors will want to understand the scope of indemnification.

The Anti-Deficiency Act generally bars "open-ended indemnity clauses" as violating the prohibition on authorizing expenditures beyond appropriated levels. Put simply, the government generally cannot agree to open-ended indemnification that might result in spending Congress has not authorized. However, federal agencies may indemnify contractors against certain claims or losses resulting from "unusually hazardous" risks. While Federal Acquisition Regulation 50.104 sets out standards and procedures for indemnification, it does not define "unusually hazardous" risks, which commonly applies to areas such as nuclear activities, advanced aerospace development and weapons deployments. Clearer guidance on the application of these protections to hazardous cyber activity may be key to harnessing the full potential of contractor support envisioned by the new strategy.

**The strategy envisions private-public partnership, not companies "hacking back."**

While the strategy suggests a greater role for companies to work with the government on offensive cyber operations, the strategy does not endorse companies taking unilateral offensive actions on their own. This is not surprising. The risks of misattribution, collateral damage and escalation are significant, and administration officials have downplayed the notion that this strategy would embrace "cyber letters of marque" to authorize private companies to go after cybercriminals and nation state adversaries on their own. In short, the rules of the road on "hacking back" remain unchanged.

Most fundamentally, the Computer Fraud and Abuse Act (CFAA) limits private companies' authority to engage in offensive cyber operations outside their own networks. The statute prohibits intentional access to a computer without authorization, which courts have interpreted extremely broadly—essentially treating such access as trespassing on another's computer system. It also prohibits knowingly causing the transmission of code that intentionally causes damage to a computer without authorization, where "damage" is defined as any impairment to the integrity or availability of data or a system. Similarly, the Electronic Communications Privacy Act (ECPA) and its subcomponents prohibit government entities and private persons from accessing or disclosing electronic communications without proper authorization.

Together, these provisions create what amounts to a blanket prohibition on most "hack back" tactics that involve accessing an attacker's systems or impairing their data, even when done in self-defense.

While defensive measures within a company's own network are generally permissible, more offensive activities can quickly raise a company's legal exposure. For example, tactics that intrusively access or monitor attackers outside the victim's network likely run afoul of the CFAA, as

do tactics like retaliatory distributed denial of service attacks or the deployment of ransomware against attackers.

The new strategy does not suggest immediate changes to this basic existing legal landscape. However, it does invite government partnerships to support a more aggressive posture within the bounds of what these existing understandings of relevant laws permit.

Companies can address many of the legal limitations through government authorization or cooperation with federal law enforcement agencies. For example, the CFAA “does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency,” suggesting certain offensive operations carried out with government authorization would not violate the statute. Meanwhile, the Cybersecurity Information Sharing Act of 2015 (CISA) authorizes private entities, for cybersecurity purposes, to “ monitor” or “operate a defensive measure” on their own information systems or those belonging to third parties, with the third party’s permission. (CISA’s definition of a defensive measure excludes any action that “destroys, renders unusable, provides unauthorized access to, or substantially harms” an information system not belonging to the private entity.)

The strategy also seeks to increase public-private cooperation and information sharing that may support joint actions under the requisite authorities. This includes leading private-sector cyber intelligence units providing the government with the type of information that can support seeking civil court orders to disrupt botnets, investigating malware operations and seizing phishing infrastructure.

WilmerHale’s Defense, National Security, and Government Contracts team has extensive experience working with companies to maximize opportunities to partner with the US government while minimizing and mitigating risks associated with participating in sensitive activities.

## *Authors*


**Matthew G. Olsen**

PARTNER

Chair, Defense, National Security and Government Contracts Practice

matthew.olsen@wilmerhale.com

+1 202 663 6359

**Joshua A. Geltzer**

PARTNER

joshua.geltzer@wilmerhale.com

+1 202 663 6404

## Erik F. Swabb

PARTNER

erik.swabb@wilmerhale.com

+1 202 663 6543

## Susan J. Hennessey

COUNSEL

susan.hennessey@wilmerhale.com

+1 202 663 6000

## Preston Marquis

ASSOCIATE

preston.marquis@wilmerhale.com

+1 202 663 6231

## Dakota C. Foster

ASSOCIATE

dakota.foster@wilmerhale.com

+1 202 663 6087