

The Clear, the Muddy, and the Insoluble of the Administration's Cyber Operations National Security Presidential Memorandum

By Leonard Bailey

The question, “Why hasn’t the private sector seized on periodic campaigns to give U.S. companies more authority to conduct offensive cyber operations against malicious cyber actors?” is a vexing one. But there is a simple answer:

C-suite executives of major companies—from CEOs and CFOs to general counsel—will not volunteer for ill-defined legal and operational risks. And over the last decade, the government has done little to resolve the uncertainty that surrounds private entities conducting offensive (and even some defensive) cyber operations, even while [proposing legislation](#) authorizing such operations.

I have [criticized](#) the Trump Administration’s [National Cyber Strategy](#) (NCS) for failing to address that uncertainty. The NCS said little about private-sector cyber operations beyond promising to “unleash the private sector by creating incentives to identify and disrupt adversary networks and scale our national capabilities.” But on August 12, the Administration released the [National Security Presidential Memorandum](#) on Expanding Capabilities to Combat Transnational Cyber-Enabled Crime (NSPM), which goes into considerably more detail than the NCS in clarifying those incentives.

The NSPM outlines a framework for augmenting the government’s cyber-operations capacity by enlisting qualified companies to conduct “Cyber Effects Operations” and “Cyber Surveillance Operations” under contract with the Departments of Justice and Homeland Security. It directs the National Coordination Center to leverage the capabilities of the private sector for conducting cyber operations against foreign cyber-enabled transnational criminal organizations. It also encourages contractors to share cyber threat information to enable operations. Per the NSPM, these contractors would act under the direction, control, and authority of the U.S. government.

Collaboration between U.S. companies and the government to combat cyber threats is not new. The U.S.

government and the private sector have had commercial arrangements involving cyber operations for many years. Some of those arrangements [reportedly](#) contracted the development of cyber analytic and forensic tools for use by federal law enforcement. Other agreements, according to [reporting](#), involved commercial cooperation with law enforcement agencies to produce spyware or exploits. U.S. military branches and the intelligence community also rely on contractors for tool and exploit development. But the NSPM encourages a different type of public-private relationship. In a break from past policy and practice, it seeks to turn private contractors into operators, the proverbial “trigger pullers” who actually execute cyber operations rather than merely furnish tools or services in support of the government.

This article asks whether the NSPM is likely to succeed in its mission to expand the U.S. government’s cyber capacity by recruiting integral private sector partners. It focuses on whether the NSPM resolves any of the uncertainty that has constrained public-private operational collaboration.

Spoiler alert: it does not. The NSPM does something more interesting but equally unproductive: it redistributes the uncertainty, instead of removing it. It is therefore unlikely to convince the most needed companies to turn their cyber operations into effective strategic tools that the government can enlist.

About the Institute for Security and Technology

The Institute for Security and Technology (IST) is the 501(c)(3) critical action think tank that unites technology and policy leaders to create solutions to emerging security challenges.

IST stands at the forefront of convening policymakers, technology experts, and industry leaders to identify and translate discourse into impact. We take collaborative action to advance

national security and global stability through technology built on trust, guiding businesses and governments with hands-on expertise, in-depth analysis, and a global network.

The “Ingenuity of the Private Sector”: Where Does It Lie?

The NSPM seeks to leverage both the “ingenuity” and the “scale, speed, and capacity” of the private sector to mount offensive cyber operations against transnational criminal organizations. But what does that mean and where in the private sector do those capabilities reside?

The private sector is not a monolith. It consists of businesses of every size, working across different industries, with highly variable appetites for risk, so it is unsurprising that some businesses eligible to participate in the NSPM are not suitable for the task. In fact, relatively few have the “scale, speed, and capacity [to] secure a critical offensive cyber advantage for the United States” that the NSPM seeks. The entities best positioned to improve the efficacy of cyber operations are specifically large information technology and communications companies with international reach.

If the government truly wants to turn disruptive cyber operations into an effective response to the cyber threats facing the United States, it should focus on strategic impact rather than tactical significance. To use cyber operations as a strategic tool—one capable of shaping cyber criminals’ decision-making and altering their behavior—such operations must have the ability to reliably generate the intended effects, the reach to operate globally, and the capacity to work at scale. In my experience, cyber operations have historically fallen short of those marks. They have proven to be useful tactical tools capable of frustrating criminals under certain circumstances, but not capable of forcing them to change their posture or deterring their behavior. In my view, it is unlikely that the NSPM will remedy this shortcoming.

The companies most enthusiastic about enlisting in the NSPM’s program will be small ones, likely staffed by former government personnel whose résumés prominently feature stints in the intelligence community or the U.S. military. The risk appetite of these companies is inversely proportional to the number of lawyers they have on staff—the fewer they have, the greater their willingness to take on risk. Those companies are capable of providing highly capable tactical cyber operations capabilities, but they do not have the capacity to reliably deliver the required effects at scale.

The companies best positioned to reliably deliver that kind of strategic impact are large, multinational telecommunications, cloud, and Internet communications providers, not boutique offensive cyber operations firms. These large providers have the technical wherewithal and positioning to block, intercept, or manipulate malicious traffic transiting their own networks with relative ease, compared to smaller companies outside the communications and information technology sectors that would need to conduct their operations on other parties’ systems using dodgy legal authority.

That said, with only a few noteworthy exceptions, multinational communications providers have been reluctant to routinely mount cyber operations because of the risks they must assume to do so—complex risks without ready answers. If the government truly wants to overcome that reticence, it should prioritize reducing uncertainty for these companies in particular, not for the broader array of potential private sector companies.

Classifying Uncertainty

Admittedly, uncertainty about risk is not the sole reason the major players have been reluctant to embrace cyber operations like those envisioned by the NSPM. But uncertainty is the throughline connecting many of industry’s reservations.

It is no secret that the private sector, particularly major providers, have been collaborating to battle cyber threats for years—both with and without government involvement. From the [2008 Conficker Working Group](#) to botnet takedowns in the 2010s to the [Log4j response](#) in 2021, companies have shown they can marshal their formidable capabilities when they perceive a need to do so. But overt, government-backed cooperation extending beyond information sharing, tool and exploit sharing, and vulnerability remediation and into technical disruption intended to hobble a cyber threat actor has not become routine.

The uncertainty that has stunted major companies’ willingness to conduct disruptive cyber operations can be grouped into four buckets, depicted below:

1. **Government backing:** Does the government, writ large, actually support private-sector involvement?
2. **Legal authority:** What law authorizes the activity?
3. **Legal protection:** Even if the activity is lawful, who bears the risk if something goes wrong?
4. **Operational risk:** What happens if there is political, commercial, or retaliatory blowback?

So how does the NSPM match up against those concerns? With apologies to Clint Eastwood, the best framing is stolen from an old-time spaghetti western, but tweaked slightly. Instead of the “The Good, the Bad, and the Ugly,” let’s examine “The Clear, the Muddy, and the Insoluble” of the NSPM.

Figure 1. Major Companies’ Uncertainty about Executing Cyber Operations



National Security Presidential Memorandum (NSPM)

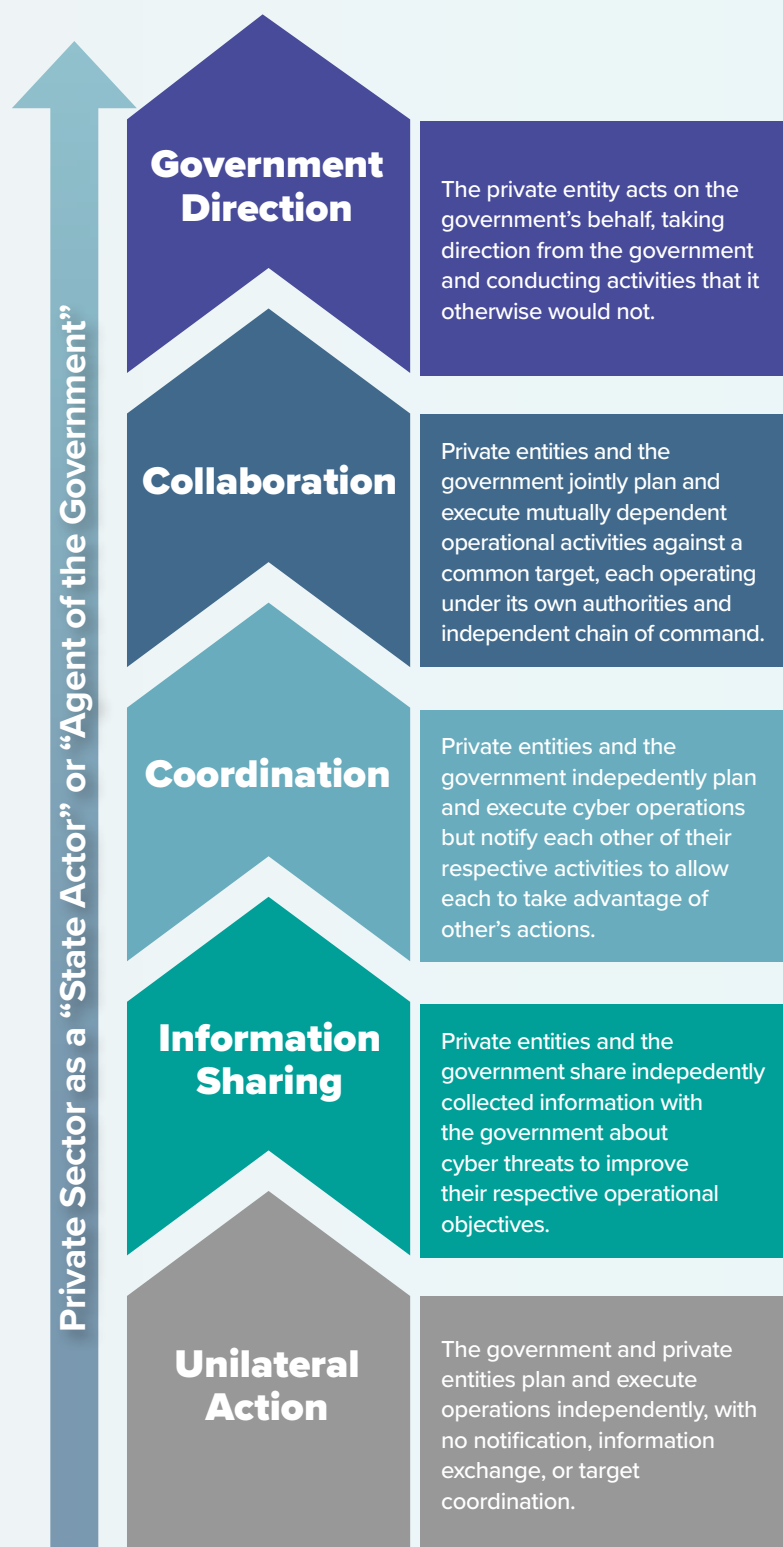


Figure 2. Models of the Private Sector's Operational Cyber Engagement with the U.S. Government

The Clear

Government Backing

The NSPM should remove any uncertainty about this Administration's support for private sector involvement in cyber operations. It is a full-throated declaration of the Trump Administration's desire to enable private sector execution of a scoped array of cyber operations: those conducted at the government's direction and against foreign cyber-enabled criminal organizations.

Going far beyond the NCS's vague pronouncements, the NSPM establishes a framework under which "Participating Companies" can enlist in government-run operations through the National Coordination Center (NCC). Within 60 days of the NSPM's release, the NCC's Directors will establish rules for oversight and direction of private sector operations, removing any doubt about U.S. government support, at least during this Administration. (Unresolved questions about longer-term government backing remain, though, because an NSPM can be rescinded by a subsequent Administration much more easily than a statute can.)

Legal Authorities

The NSPM also squarely addresses the question of legal authorities. As illustrated in Figure 2, there is a spectrum of public-private collaboration in cyber operations.

The more enmeshed the government and private parties become, the more likely a private party's actions will be attributed to the government. There is no Rubicon marking precisely when a private party becomes an instrument of the government or a government agent. The analysis is fact-specific, depending on factors like the government's degree of control over a private party's actions, whether those actions are taken solely to benefit the government, and how much discretion the party retains. Legal analysis of the status of a private actor engaged in information sharing or close coordination with the government is usually demanding, but the NSPM makes that determination much easier.

[Section 2\(a\)\(i\)](#) of the NSPM mandates that Participating Companies will operate under government direction and rely upon government authorities, placing them decisively at the far extreme of this spectrum of government control. Presumably, the NSPM's drafters anticipate that this will mean speedy, streamlined, and seamless execution of cyber operations consistent with government objectives, although the written approval of plans,

interagency deconfliction, and legal review required by the NSPM belies that expectation. Regardless, companies will not decide for themselves whether, when, and how to conduct a disruptive operation. Instead, government approval of their operations will presumably be based on a common set of government priorities, which should simplify planning and execution.

The legal consequences of this relationship will be complicated. Government direction may create an avenue for a contractor to claim certain legal defenses, but it doesn't automatically grant a contractor every legal protection available to the government, nor make every action of a contractor an action of the government.

Still, the combination of government contracts and operating under government direction may unlock helpful, otherwise unavailable legal protections for participating companies. Unfortunately, exactly which defenses apply, and whether gaining one defense means sacrificing others, is much muddier.

The Muddy

Liability Protections ... Kinda

As a matter of law, the NSPM cannot simply declare a private company immune from liability under statutes or doctrines controlled by Congress or the courts—nor does it try to do so. The NSPM is silent about liability protections. Instead, intentionally or not, it places government contractors in a position to invoke existing statutory exceptions and assert common-law defenses. Unfortunately, those protections do not all operate the same way, and some may not be a good fit for cyber operations at all.

Two sets of legal rules are particularly important here: section 1030(f) of the [Computer Fraud and Abuse Act](#) (CFAA) and the contractor defenses associated with [Boyle v. United Technologies Corporation](#), and [Yearsley v. W.A. Ross Construction Company](#). A full treatment of these defenses can be found in the Appendix, and they are summarized below.

Cyber operations like those contemplated by the NSPM implicate the CFAA, the federal anti-hacking statute. The CFAA generally prohibits unauthorized access to a computer, whether by private parties or the government, but section 1030(f) of the CFAA exempts lawfully authorized investigative, protective, or intelligence activity conducted by federal law enforcement or intelligence community agencies. Whether that exemption extends to a private contractor acting under a federal agency's direction is unsettled, but there are reasons to doubt that an exemption for a contractor can be inferred simply because a contractor is acting as the government's agent. A comparison to other statutes and canons of statutory interpretation suggests it may not.

Even so, common law public authority and entrapment-by-estoppel defenses may provide a viable alternative to a 1030(f) exemption that would protect contractors. The application of those defenses to CFAA-type violations, however, leaves unresolved questions about what statutory authorization the government must have before it can confer its authority on a private actor.

As for civil protections from potential tort liability, Boyle and Yearsley offer contractors two different doctrines that shield them from tort claims. However, they provide defenses, not immunity, meaning they do not necessarily prevent a costly lawsuit, discovery, or trial. And even more important for cyber operations, legal cover depends entirely on the scope of the government's authorization and the contractor's adherence to it. A cyber operator who needs to adapt in real time to an unexpected operational contingency or crafty adversary—which would not be unusual—risks straying from what the government has authorized, therefore jeopardizing its legal protections.

There may also be a less obvious cost to acting under the government's direction. A contractor may gain legal protections for government-directed activities at the expense of legal protections Congress made available specifically and exclusively to private entities. The Cybersecurity Information Sharing Act of 2015 and the "rights or property" exception to federal surveillance statutes, such as those found in the [Wiretap Act](#) and [Stored Communications Act](#), are two examples of this potential quandary.

The NSPM removes uncertainty about whether the government wants private operational help, but not about the legal consequences of providing it.

The Insoluble

I have reserved the "Insoluble" for problems that an NSPM, and perhaps even an act of Congress, cannot fully solve. Once a participating company targets a foreign information system, it will confront legal and commercial risks that cannot be displaced by U.S. laws.

The first challenge is a conundrum created by the NSPM itself. [Sections 2\(a\)\(i\) and 2\(b\)](#) of the NSPM require operations to be conducted "pursuant to the Federal Government's lawful authorities" and consistent with applicable law and international obligations. But some fundamental rules about cross-border operations remain contested within the international community, including the application of the principle of sovereignty to accessing foreign systems.

Swiss law illustrates the conflict well. Swiss authorities claim that Swiss sovereignty is implicated whenever foreign law enforcement accesses a server there, bypassing established mechanisms for international legal assistance. More pointedly, [Article 271](#) of the Swiss Criminal Code

criminalizes carrying out, without authorization, activities on Swiss territory on behalf of a foreign state. A U.S.-directed cyber operation against a server in Switzerland could, therefore, raise [Article 271](#) concerns, depending on how Swiss authorities interpret the conduct. What exposure does a participating company face when it disrupts a server in Switzerland at the U.S. government's direction and risks violating Swiss law? The NSPM does not resolve this conflict.

Layer on top of that the sheer number of jurisdictions the NSPM's operations could implicate. The NSPM targets foreign criminal groups, so NSPM cyber operations will almost invariably operate against systems in other countries. UN Trade and Development's [Cyberlaw Tracker](#) currently reports that 90 percent of the 195 countries it tracks have enacted cybercrime legislation. The odds are good that a contractor executing an operation under the NSPM may encounter or potentially violate another country's laws.

A participating company also faces the commercial and operational risks of being perceived as an arm of the U.S. government. A company known to be conducting cyber operations on behalf of the government may end up handicapped in foreign markets where its cooperation with the U.S. government will not be viewed charitably. For example, U.S. companies perceived to be in close collaboration with the U.S. government faced backlash in the EU and elsewhere following enactment of the [U.S.A. Patriot Act](#). And the disclosures of [Edward Snowden](#) helped propel the [General Data Protection Regulation](#) forward and triggered litigation that led the EU's top court to [strike down](#) the transatlantic data-transfer framework that facilitated U.S. companies' ability to obtain EU data.

And while U.S. legal defenses may shield participating companies in U.S. courts, they do not provide a safeguard against liability under foreign laws or proceedings in foreign courts. The U.S. government can authorize an operation and provide whatever protections U.S. law allows, but it cannot immunize a contractor from the laws of the foreign countries in which operations will be executed. This creates an odd asymmetry between the government, which gets the private sector's operational capability, and the company, which bears potential legal exposure under foreign laws.

Keeping the company's identity confidential might reduce some of these risks, but the blowback from a leak of undisclosed government ties could prove even worse than open acknowledgement. Targeted criminal organizations may also retaliate against participating companies, believing U.S. companies can be intimidated or punished in ways the U.S. government cannot.

The Cost-Benefit Analysis

The NSPM does not reference letters of marque and reprisal, which are constitutionally authorized commissions entitling bearers to sink or capture vessels belonging to enemy nations. Indeed, [Administration officials](#) have sought to distinguish the Administration's cyber policies from letters of marque. Setting aside the [criticism](#) of using letters of marque to combat cyber threats, letters of marque had at least one helpful feature the NSPM lacks: a clear commercial model.

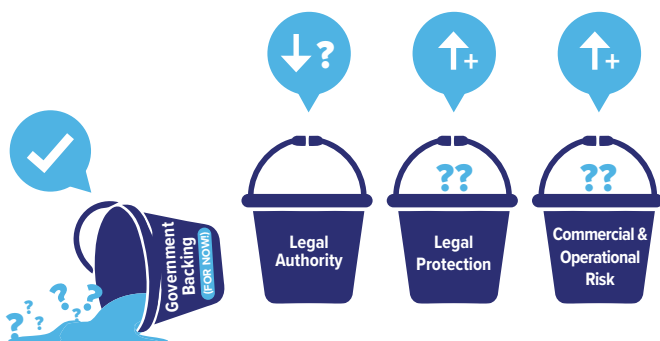
In the 1800s, when letters of marque were last issued, a vessel, cargo, or other [property](#) captured in an armed conflict was subject to "prize law," so named because goods captured during an armed conflict were called "the prize." Authorized privateers were allowed to keep enemy vessels or goods as compensation for their work.

The NSPM does not discuss compensation, but other than operations targeting crypto wallets, cyber operations under the NSPM are unlikely to furnish contractors with opportunities to seize valuable property. (In any event, seizure of crypto wallets by government agents would raise interesting legal questions about forfeiture law that may confound a contractor's ability to claim such booty.) Thus, NSPM contractors will presumably be compensated primarily by the Treasury Department.

But how sizable a paycheck would a major company facing indeterminate inadequate legal protections, operational risks, and loss of customers in foreign markets demand? In addition, how much compensation should they receive to account for the burden of government review of their security, personnel, and preparedness?

We will need to wait until the first contracts are signed to find out what the payouts will be. Even so, while there may be no simple way to arrive at a definitive figure, based on SEC filings two major U.S. telecom companies had non-U.S. revenue in 2025 of approximately [\\$5.4 billion](#) and [\\$2.5 billion](#), respectively. The world's largest software maker, which is also an international communications provider, states in its [Annual Report](#) that it earned \$137.1 billion from non-U.S. customers in fiscal year 2025. Thus, a premium price will likely be needed to motivate the most impactful companies—like the international communications providers readily able to conduct on-net operations—to overcome their reticence, raising questions about cost-effectiveness.

Figure 3. NSPM's Impact on Major Companies' Uncertainty



Conclusion

The NSPM advances the debate over the private sector's role in cyber operations by committing to a model for cyber operations, thereby giving proponents and critics a concrete example to interrogate. The NSPM decisively settles one question, at least for this Administration.

The government is championing the use of the private sector's operational capabilities to augment its own and welcomes private sector collaboration under the terms of the NSPM. And by requiring participating companies to operate under government direction, it gives companies a concrete, albeit untested, operational framework that had previously been lacking.

However, harder questions remain unresolved. Boyle's legal defenses for contractors have traditionally applied to companies that build widgets, hardware, or military equipment to precise government specifications. Cyber operations against sophisticated cyber criminals may prove harder to capture in contractual language while preserving a contractor's defenses. Such operations often depend on the ability to improvise and adapt—sometimes on the fly—which may challenge existing contractor defense doctrine that requires contractors to adhere closely to government direction. Furthermore, underlying any question of liability is the question of how a contractor can handle exposure to foreign laws that no U.S. liability defense can mitigate.

The forthcoming NSPM protocols may establish the rules of operation, but they are unlikely to fully resolve such questions.

Returning to the buckets of uncertainty, government backing is solved, at least for now. Legal authority and liability, on the other hand, are only partially addressed. Companies are left to cobble together an unwieldy assemblage of conceptually applicable but untested legal defenses into a claim for liability protection.

Erasing the doubts harbored by critical industry partners will require legislation that affirmatively allows the government to delegate its operational role to the private sector, authorizes the private sector to execute cyber operations, and grants the private sector immunity—rather than just defenses—for conducting operations consistent with government direction. Getting such legislation enacted would likely require a coordinated campaign by both government and industry, along with the expenditure of significant political capital, but the payoff would be removing a major impediment to buy-in from vital major companies.

Even with legislation, commercial and operational risks would still remain. The larger companies arguably best positioned to satisfy the objective of augmenting operational “scale, speed, and capacity” may not be easily enticed to operate under the NSPM. Their reasons could vary: for instance, they may already have arrangements with the U.S. government and be uninterested in renegotiating them to conform to the NSPM or they do not wish to operate in this field at all, regardless of the compensation. And even though a handful of smaller firms—including some recent [startups](#) focused on providing offensive cyber services to the government—may be undeterred and prepared to put their misgivings aside for NSPM contracts that are lucrative enough, will they be prepared to provide the type of capacity at the scale the government is seeking?

Even after the government and prospective contractors successfully navigate this gauntlet of uncertainties, the intractable problem of exposure to foreign laws remains, and that risk alone could be a deal breaker.

Ultimately, the NSPM has not eliminated uncertainty. Instead, companies considering signing contracts under the NSPM may move from asking, “May we do this?” to the harder question: “What happens to us if we do?” The impact of the NSPM will prove to be blunted without a clear answer.

About the Author

Leonard Bailey spent 33 years at the Department of Justice, where he managed cyber policy as an Associate Deputy Attorney General, Senior Counselor to the Assistant Attorney General of the National Security Division, and Head of the Cybersecurity Unit and Special Counsel for National Security in the Criminal Division's Computer Crime and Intellectual Property Section. He is a graduate of Yale University and Yale Law School.

The Institute for Security and Technology and the authors of this report invite free use of the information within for educational purposes, requiring only that the reproduced material clearly cite the full source. This report is written and published in accordance with the Institute for Security and Technology's [Intellectual Independence Policy](#). The authors are solely responsible for its analysis and recommendations. The Institute for Security and Technology and its supporters do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

Legal Protection Under the Private Cyber Operations NSPM: What Do Contractors Actually Get?

Introduction

The main article briefly summarizes the liability protections the [National Security Presidential Memorandum on Expanding Capabilities to Combat Transnational Cyber-Enabled Crime](#) (NSPM) may afford contractors who enlist in the NSPM's program. This appendix provides a more robust analysis of those liability protections and their challenges. The following legal analysis examines the statutory exceptions to the [Computer Fraud and Abuse Act](#) (the CFAA, 18 U.S.C. § 1030) and the defenses provided to contractors by common law to assess whether the NSPM's contract requirement offers companies who sign a contractual agreement with the government sufficient protections to shield them from civil or criminal liability under U.S. law.

[Section 2\(a\)\(i\)-\(ii\)](#) of the NSPM requires "Participating Companies" to contract with the Departments of Justice and Homeland Security and conduct cyber operations under government direction. As outlined below, companies that contract with the government under the NSPM will confront several branching questions about liability protection, some of which are novel and, to date, unanswered. Government contractor status may unlock legal defenses that, while untested in the context of cyber operations, could provide them with meaningful legal protection.

But even if a company that contracts with the government succeeds in raising those defenses, it may still endure a costly trial and civil discovery before escaping liability. What's more, those defenses could jeopardize other protections that companies generally enjoy.

The problem is not simply that these defenses are untested in cyber operations. Their requirements may conflict with the real-world execution of cyber operations. Some legal protections require strict adherence to government instructions. Cyber operators, by contrast, often need to adapt when targets move, infrastructure changes, or unexpected effects emerge. Crucially, the more the execution of an operation strays from the government's instructions or the more discretion an operator exercises, the harder it may become to demonstrate in legal proceedings that the contested conduct was authorized by the government and, therefore, legally protected.

This appendix reviews relevant doctrine, examines the potential consequences of becoming a government-directed contractor under the NSPM, and explores steps that could put private sector participation in a program such as this on better legal footing.

Theories of Liability Protection for Government Contractors

The analysis starts with the statute most likely to be implicated by the disruptive cyber activities contemplated by the NSPM the [Computer Fraud and Abuse Act](#) (CFAA), the principal federal hacking statute.

Extending the CFAA's Statutory Exemption to Private Actors

Anyone executing "Cyber Effects Operations" under the NSPM— that is, manipulating, disrupting, denying, degrading, or destroying information systems or data— could face civil and criminal liability under the [CFAA](#). But section 1030(f) exempts state and federal law enforcement agencies and federal intelligence agencies from the CFAA's prohibitions when they engage in lawfully authorized investigative, protective, or intelligence activity. A DOJ or DHS law enforcement agency conducting a legitimate criminal investigation should satisfy section 1030(f)'s "lawfully authorized" requirement. A government contractor hired to support such a law enforcement agency and strictly operating under that agency's direction arguably should also be eligible for 1030(f)'s exception, but there is reason to question whether section 1030(f)'s exemption can be extended to non-governmental actors at all.

Section 1030(f) refers exclusively to state and federal government entities. It does not expressly mention agents of the government or non-governmental actors. Thus, courts might interpret 1030(f)'s scope to be institutional, not relational, meaning the exemption would solely cover the activities of identified law enforcement and intelligence agencies, not private actors acting in support of those agencies.

Whether section 1030(f) can extend to private actors is an unsettled legal question. Case law and legislative history for section 1030(f) are practically nonexistent. As a result, this analysis focuses heavily on the statutory text and how courts might interpret it.

Pure textual arguments appear to support a narrow reading of the exception. Arguably analogous federal statutes that exempt private actors from statutory prohibitions do so explicitly. Section 1201(e) of the [Digital Millennium Copyright Act's](#) law enforcement exemption, for example, expressly refers to “an officer, *agent*, or employee of the United States” (17 U.S.C. § 1201(e)) (Emphasis added.) The [Wiretap Act](#) includes several exceptions for private parties acting “under color of law,” “agents,” “under a contract with the government,” and “under the supervision of an investigative or law enforcement officer authorized to conduct the interception.” While the omission of such language from section 1030(f) is not conclusive, it may give a court reason to doubt that section 1030(f) covers contractors.

Courts have sometimes interpreted government-specific exclusions narrowly in the absence of explicit language. For instance, the court in [In re Capitol Breach Grand Jury Investigation Within District of Columbia](#), reasoned “a private international firm like Deloitte that simultaneously holds multiple contracts with private and public entities across the globe ... cannot be considered a government ‘employee’ in any meaningful sense.” It therefore ruled that the contractor was not “government personnel,” and therefore not entitled to exemption from the grand jury secrecy rule.

The canons of statutory interpretation also include a rule that is instructive, although not dispositive: when Congress expressly includes private actors in one statute but omits them from another, a court may infer that the omission was deliberate. This interpretative rule is not controlling and is most compelling when comparing terms within the same statute rather than across arguably similar statutes. Nevertheless, in applying this rule, a court could infer that Congress’ omission of non-governmental personnel acting as agents of the government from section 1030(f) was deliberate and bars them from the exemption.

None of this makes a narrow reading of section 1030(f) inevitable, but it should be factored into the calculus a contractor makes when weighing risks under the CFAA.

How wary should a contractor be of not being protected by 1030(f)? The odds of a government-directed contractor being charged with violating the CFAA after faithfully executing a lawful government operation seem remote.

On the other hand, CFAA-based civil liability remains a concern, because section 1030(g) provides a civil cause of action for CFAA violations. In other words, without section 1030(f)’s exemption, a contractor would face unmitigated risk of civil liability. There are, however, common law defenses that may also protect a government contractor sued for actions taken under the NSPM.

Spotty Common Law Defenses to CFAA Liability

Even if ineligible for section 1030(f)’s exemption, a government contractor may turn to common law defenses not found in statutory text to evade civil and criminal liability under the CFAA. The “public authority” defense and “entrapment-by-estoppel” are based on the same set of facts: a private party who knowingly violates a federal criminal law while relying on the authorization of a governmental official. They also share a common equitable theory: a private party who reasonably relies upon a government official’s directions should not be subjected to government sanction.

In [Naicom Corp. v. Dish Network Corp.](#), an unpublished but affirmed district court decision that most squarely addresses the public authority defense in proceedings involving the CFAA, the court dismissed a CFAA claim against private parties who assisted in executing federal search warrants on plaintiffs’ computers. But the court relied on the existence of a warrant, not supervision by the FBI agents present during the search, to conclude that the private parties’ conduct was “lawfully authorized.” Therefore, while this common law defense may offer an alternative to the 1030(f) exemption, its application could be limited to instances where the putative CFAA violation was authorized by a warrant or similar legal authority. This particular scenario is likely to occur only rarely under the NSPM, because most operations will target foreign computers located beyond the jurisdiction of U.S. courts. While the *Naicom* case does not foreclose application of the public authority defense, it does represent a potential limitation.

Unlike the public authority defense, “entrapment-by-estoppel” is grounded in Due Process. But much like the public authority defense, it is premised on a private party’s reasonable dependence on government authorization. The (contested) difference between the two defenses is entrapment-by-estoppel’s dependence on “apparent authority” and the public authority defense’s reliance on “actual authority.” Apparent authority involves the advice of a government official who reasonably appears to have the power to authorize the conduct but in fact lacks such legal authority. Actual authority, on the other hand, is implicated when a government official responsible for interpreting or enforcing the relevant law gives erroneous advice. The less restrictive requirement of entrapment-by-estoppel’s apparent authority standard makes it a more colorable legal defense to a CFAA charge.

However, when it comes to *civil* liability, federal courts have not recognized entrapment-by-estoppel as a valid defense, because the defense is rooted in Due Process guarantees for criminal proceedings. As theorized earlier, criminal prosecution is unlikely to be the primary concern for a contractor acting under government’s direction. Defenses to claims of tort liability must be found elsewhere.

Contractor Defenses: Protection Possibly But Definitely Not Immunity

By requiring Participating Companies to enter into government contracts, the NSPM provides them with a potential path to other common law defenses available against some tort claims. The two most relevant doctrines are articulated in [Boyle v. United Techs. Corp.](#), 487 U.S. 500 (1988), and [Yearsley v. W.A. Ross Construction Co.](#), 309 U.S. 18 (1940), each providing its own version of a government contractor defense.

In [Boyle](#), the Court held that federal law could displace state tort law when a uniquely federal interest is implicated and when there is a significant conflict between that federal interest and state law. [Boyle](#) established a three-part test used to determine whether a government contractor is eligible for this defense that preempts state tort claims:

1. The government must have approved reasonably precise specifications.
2. The equipment or services furnished by the contractor must have conformed to those specifications.
3. The contractor must have warned the government of dangers associated with its execution of the contract that it knew but that the government did not.

Yearsley offers a similar contractor defense under a different theory. *Yearsley* protects a contractor sued for doing what the federal government lawfully authorized it to do, but only when the contractor's conduct was within the scope of that authorization. Accordingly, courts have found that a contractor who exceeds government authority or deviates from government specifications cannot claim the defense.

In the Supreme Court's 2026 decision in [GEO Group, Inc. v. Menocal](#), the Court refined *Yearsley*'s rule by clarifying that *Yearsley* provided a "merits defense" and not "derivative sovereign immunity," as some courts had held. The difference between the two is significant. Sovereign immunity means no court possesses the power to adjudicate the case at all, and the defendant is entitled to be free from all burdens of litigation, regardless of what it did and whether it violated the law. A merits defense, on the other hand, allows a defendant to escape liability, but it permits a court to exercise jurisdiction over the matter and therefore does not allow a defendant to avoid litigation altogether. A defendant can feasibly evade liability with a merits defense, but only after proving that its conduct was lawful, justified, or otherwise did not satisfy the elements of the plaintiff's claim. Doing so may require costly motions practice, discovery, and trial.

The realizable benefits of *Boyle*'s and *Yearsley*'s defenses are dubious. They can be costly to secure and may be difficult to secure at all under real-world conditions. As discussed further below, the faithfulness to government instructions required to secure legal protection can be at odds with the adaptability often required to execute cyber operations successfully. Contractors and the government may at times be forced to choose between optimizing liability protection and achieving operational success.

Operationalizing Boyle and Yearsley

Boyle may ultimately not be a reliable vehicle for shielding contractors performing cyber operations from liability. It provides the strongest defense when a government contract includes precise instruction concerning the challenged conduct. A contract that, for example, merely directs a contractor to "disrupt transnational criminal organizations online" leaves the contractor with plenty of discretion—probably too much for *Boyle*.

Thus, *Boyle* tees up a line-drawing question: "How much discretion can a contractor exercise before the conduct being challenged is no longer the conduct the government directed?" This question is particularly important in the context of the NSPM. Cyber operators routinely need to pivot, improvise, and work around unexpected obstacles, which will complicate the ability to draw boundaries between conduct that was specifically directed and, therefore, protected, and conduct that is not and will not support a defense under *Boyle*.

The Supreme Court's 2026 decision in [Hencely v. Fluor Corp.](#), 608 U.S. ____ (2026), is instructive. *Boyle* does not protect a contractor from liability for conduct the government did not order or authorize, but *Hencely* did not find that every exercise of discretion undermines the defense. The challenged conduct must actually conflict with a federal directive or policy to lose its preemptive authority. On the other hand, *Boyle*'s preemptive authority does not protect a contractor when the government contract is silent about the complained-of conduct.

In applying *Boyle* to cyber operations, a contract may need to specifically identify the target, permissible methods, timing, geographic scope, and operational boundaries with enough detail to demonstrate that a contractor's conduct was actually directed by the government. Yet, a contractor may seek to avoid instructions that spell out every single detail, because a too-detailed set of instructions will increase the odds that a contractor's actions deviate from government instructions and may also narrowly constrain the contractor's ability to complete the mission.

Yearsley's doctrine may be a better fit for cyber operations, as it appears to be more permissive. It asks whether the government validly authorized the contractor's conduct and whether the contractor stayed within the ambit of that authorization, shifting attention from whether every operational step was spelled out in the contract to whether the contractor was carrying out the legally authorized mission when the allegedly tortious conduct occurred.

Yearsley has its own challenges, though. The viability of the defense depends on whether Congress actually authorized the government to perform the underlying task *and to delegate it to a private contractor*, raising an issue reminiscent of the 1030(f) exception discussed earlier. If statutes do not clearly grant the government the authority to delegate the underlying act to a non-governmental party, a contractor may have difficulty showing that the government validly conferred the authority it was exercising. The absence of express congressional authority to delegate cyber-operational powers to private entities could prove to be problematic.

Furthermore, staying within the scope of the government's lawful authorization will also require a government contractor to exercise diligence. In [*GEO Group, Inc. v. Menocal*, 607 U.S. ____ \(2026\)](#), the Court emphasized that *Yearsley* only protects a contractor when it has received lawful authorization and acted within its terms. Errors or flawed execution of an operation might raise questions about whether a contractor operated as the government directed. In [*In re U.S. Office of Personnel Management Data Security Breach Litigation*](#), the court concluded that a government contractor sued for a data breach could not claim it performed as the government directed because OPM did not authorize or direct it to design its systems with the security flaws that led to the breach.

Using the same reasoning, a government contractor sued for disrupting the communications of innocent businesses after deciding to sinkhole a block of IP addresses to disrupt a targeted server with a shared IP address might lose its protections under *Yearsley*, because the government did not direct it to target innocent businesses. Mistakes may happen, but *Yearsley* may not be helpful when they do.

Loss of Existing Legal Protections?

Another less obvious question posed by acting under government direction is whether it jeopardizes protections that Congress gave companies precisely because they are private entities. [The Cybersecurity Information Sharing Act of 2015](#) (CISA 2015, which Congress recently reauthorized until December 11, 2026) is a prime example. In the legislation, Congress conferred cybersecurity authority on "Non-Federal Entities" that intentionally excluded the government, or "Federal Entities" under CISA 2015.

CISA 2015 contains definitions distinguishing between Non-Federal and Federal Entities, and the cybersecurity authorities the statute provides in section 1503 only apply to the former. The omission of Federal Entities from section 1503 was intentional. When CISA 2015 was enacted, the storm created by the disclosure by Edward Snowden about government surveillance programs had not subsided. Privacy advocates and parts of the tech industry [attempted to block it](#) as it gained momentum. Congress, wary of giving the government what might be perceived to be new surveillance authorities, crafted the law to grant information sharing authority only to private entities.

So, companies working with the government may find themselves in a bind. They may gain access to contractor defenses, while simultaneously compromising their eligibility for authorities Congress designed expressly for the private sector.

Electronic communications services providers face a similar quandary concerning cybersecurity activities conducted under the "rights or property" exceptions in federal surveillance statutes: the Stored Communications Act (18 U.S.C. [2702\(b\)\(5\) and \(c\)\(2\)](#)) and the Wiretap Act (Section 2511(2)(a)(i)). Those provisions permit providers, in specified circumstances, to monitor, intercept, or disclose communications to protect their own rights or property. [Courts have found that providers are not acting to protect their rights or property when law enforcement is directing the provider's actions and the provider is acting only to further law enforcement's interests.](#)

Therefore, government direction may create some legal benefits but possibly at the expense of others.

Other Existing Legal Protections

Some electronic surveillance statutes contain legal defenses for communications providers engaged in executing legal processes like subpoena, orders, or warrants, or for operating pursuant to other congressionally furnished authority. For example, a provider that discloses electronic communications to a law enforcement agency pursuant to a Stored Communications Act (SCA) warrant may claim the defense of "good faith" reliance on that warrant. 18 U.S.C. 2707(e). If proven, a participating company would have a complete defense to any civil or criminal action brought under the SCA. The Wiretap Act contains a similar provision, 18 U.S.C. 2520(d).

These protections have limits, though. They are only available to providers of wire or electronic communications services and mostly cover activities the NSPM defines as “Cyber Surveillance Operations,” which mainly involve the intelligence collection rather than “Cyber Effects Operations.” Furthermore, while the NSPM anticipates the potential of needing such legal process (Sec. 3(a)(xi)), cyber operations under the NSPM may not typically be conducted pursuant to court orders. Cyber operations requiring legal process may prove to be incompatible with the NSPM’s goal of increasing the speed and tempo of cyber operations.

NSPM Example: Hacking Corp.

How might a participating company assess its legal exposure for conducting cyber operations under the NSPM? Imagine Hacking Corp. signs a contract with the DOJ under the NSPM to disrupt servers in South America as part of a sanctioned cyber operation against a criminal organization engaged in large-scale eldercare fraud.

Before signing the contract with DOJ to conduct this operation, Hacking Corp. may seek answers to an array of questions to assess its legal risk:

- » **Statutory Authorization:** Does the government have legal authority to direct Hacking Corp. to take down servers in South America engaged in such activity?
- » **Contractor Status:** What is Hacking Corp.’s legal relationship with the government and is it properly established by contract?
- » **Liability Protection under *Boyle*:** Did the United States provide reasonably precise directions for how, when, and where the takedown operations should be conducted; can Hacking Corp. follow those directions and complete the mission; if not, would any additional actions taken to successfully complete the operation conflict with its instructions; and does Hacking Corp. know of any dangers of conducting the operations that are unknown to the government?
- » **Liability Protection under *Yearsley*:** Did Congress grant the government the authority to conduct such operations and to delegate its authority to a private actor; did the government validly authorize Hacking Corp.’s conduct; can Hacking Corp. stay within the scope of that authorization to complete the mission; if not, would any additional actions taken to successfully complete the operation take it outside the government’s authorization?
- » **Legal Defenses under the CFAA:** Is DOJ lawfully authorized to take down the servers for a law enforcement, protective, or intelligence purpose; will Hacking Corp. be able to conduct the mission consistent with DOJ’s direction; if not, would any additional actions taken to successfully complete the operation conflict with DOJ’s directions; and did DOJ obtain judicial or other legal authority to take down the servers?
- » **Other Common Law Defenses:** Is Hacking Corp. relying on DOJ’s direction to take down these servers; and does DOJ have the actual authority to render that advice?
- » **Other concerns:** Will the operation violate the laws of the countries in which it will be conducted; and is the operation being conducted with notice to or consent of those countries?

A detailed government contract that specifies the targets, methods, circumstances, and operational boundaries should leave the company in a strong position under *Boyle* and *Yearsley*. Details may matter, though. May Hacking Corp. use a different tool if it turns out a server is not configured as anticipated? What if the targeted server unexpectedly moves to a different cloud provider located in a different country? How should the discovery of additional infrastructure after gaining access to the target server be handled?

A contract that simply states “disrupt servers operated by transnational criminal organizations in South America” leaves substantial room for operational judgment, and *Hencely* makes clear that *Boyle* does not protect contractor conduct that the government did not expressly order or authorize. This does not necessarily mean the company is forbidden from improvising, but any act that is challenged in the future will need to be linked to the government’s authorization.

If the instructions are vague or if Hacking Corp. believes the specified instructions will not result in a successful takedown, Hacking Corp. may seek to amend the contract. Should the operation result in a lawsuit, undocumented, on-the-fly corrections may support the mission but could make it harder to show that the government actually directed any conduct that is later challenged.

Section 1030(f) will exempt the DOJ's authorized law enforcement activities specified in the statute. The case for extending that exemption to Hacking Corp. will be strongest if Hacking Corp. avoids exercising any operational judgment and strictly follows the DOJ's directions. The further it strays from DOJ orders, the more questionable its claim for a 1030(f) exemption. This assumes that the DOJ may in fact lawfully extend its exemption under 1030(f) to Hacking Corp. at all, a matter that appears unsettled in case law. The defense of the exemption would be bolstered if DOJ has obtained a warrant or other legal process, but that is unlikely in this case because U.S. courts will likely not have jurisdiction over these activities occurring abroad.

And, of course, Hacking Corp. must avoid making errors, because a mistake may bar its legal defenses altogether. *Hencely* and *GEO Group* hold that contractor's defenses only cover actions the government actually directed, and *In re: U.S. Office of Personnel Management Data Security Breach Litigation* suggests that flawed execution of a contract may mean, *per se*, that the contractor's actions were not authorized by the government.

Bringing Greater Certainty to the NSPM's Legal Protections

This hodge-podge of statutory and common law defenses provides a stew of legal protections that lacks legal clarity. While some of these protections provide colorable defenses to lawsuits, they vary in scope and certainty. And even the legal protections most likely to prevail provide something less than "immunity," leaving contractors vulnerable to time-consuming and costly discovery, motions hearings, and possibly even a trial before escaping liability.

Engineering more robust legal protection may be the most critical step that someone seeking to convince companies to sign onto the NSPM could take. This can be accomplished by amending existing laws or enacting brand-new legislation. In either case, making legal protections as explicit and as unconditional as public policy allows should be the goal. But what might such legislation look like?

Clarifying government contractor liability under the CFAA is arguably the easiest fix: just adding the words "agent or government contractor" to section 1030(f)'s list of eligible parties would resolve any doubt about the exemption's coverage. There are many options for extending government contractor protection from tort liability, but the most direct, effective change would be to enact a standalone statute providing immunity—rather than a mere legal defense—to lawsuits for government-authorized conduct.

Congress could look to other federal statutes that expressly confer immunity for examples of language that would provide stronger protection. A statute could, for example, expressly provide that a private contractor acting within the scope of a federally authorized cyber operation is not liable under specified federal and state causes of action. However, using the word "immunity" provides stronger legal protections. Statutes like the [PREP Act](#) state that a covered person "shall be immune from suit and liability." Other statutes like the [Foreign Sovereign Immunities Act](#) provide immunity by stripping U.S. courts of jurisdiction with language like, "[A party] shall be immune from the jurisdiction of the courts." By contrast, statutes that merely bar causes of action or prohibit the imposition of liability without expressly barring the suit itself — such as [Section 230](#)'s "no cause of action may be brought" — may be construed as conferring only a liability defense, not an immunity from suit.

Conclusion: A Defense You Can Raise, Not a Guarantee You Can Rely On

Where does this "muddy" analysis—referring back to the original "The Clear, the Muddy, and the Insoluble" framing—leave a company considering a contract under the NSPM? If a government contract specifies its particulars with precision, the company may have meaningful protections under *Boyle* and *Yearsley*, assuming the contractor follows those directions and delegation authority (under *Yearsley*) and an exemption under 1030(f) exists in the first place.

But if a contract outlines a vague grant of authority that leaves contractors to improvise, those defenses become weaker the further the company strays from government instructions.

The NSPM has not yet matched up the legal protections available to contractors with the realities of cyber operations. Maybe that coordination will come when the NSPM's protocols are drafted by the National Coordination Center. The primary tension is between doctrines, which reward precision about government authorization, and cyber operations, which often require adaptability.

Until contracts—and eventually courts and possibly Congress—draw the line between permissible operational discretion and conduct that falls outside the government's authorization, companies will need to weigh their appetite for risk against the benefits of enlisting in the NSPM's program by using their best judgment. The NSPM gives companies interested in signing up something valuable: clear government backing and forms of government authorization. But authorization is not the same thing as established legal protections or immunity. Existing legal protections mostly provide defenses that must be litigated, not the certainty many companies may want beforehand.