

MAYER | BROWN

THE NEW ACTIVE CYBER DEFENSE

Administration Strategy and Considerations for the Private Sector

Tuesday, October 27, 2026

TODAY'S SPEAKERS



PARTNER

ADAM HICKEY

MAYER BROWN



PARTNER

STEPHEN LILLEY

MAYER BROWN



CHIEF LEGAL OFFICER

SUJIT RAMAN

TRM LABS

AGENDA

1. Overview of the August 2026 NSPM
2. History: PPD-20 and NSPM-13
3. Regulatory Context: CFAA, FISA, and Related Laws
4. Considerations for Companies Moving Forward
5. Questions & Discussion

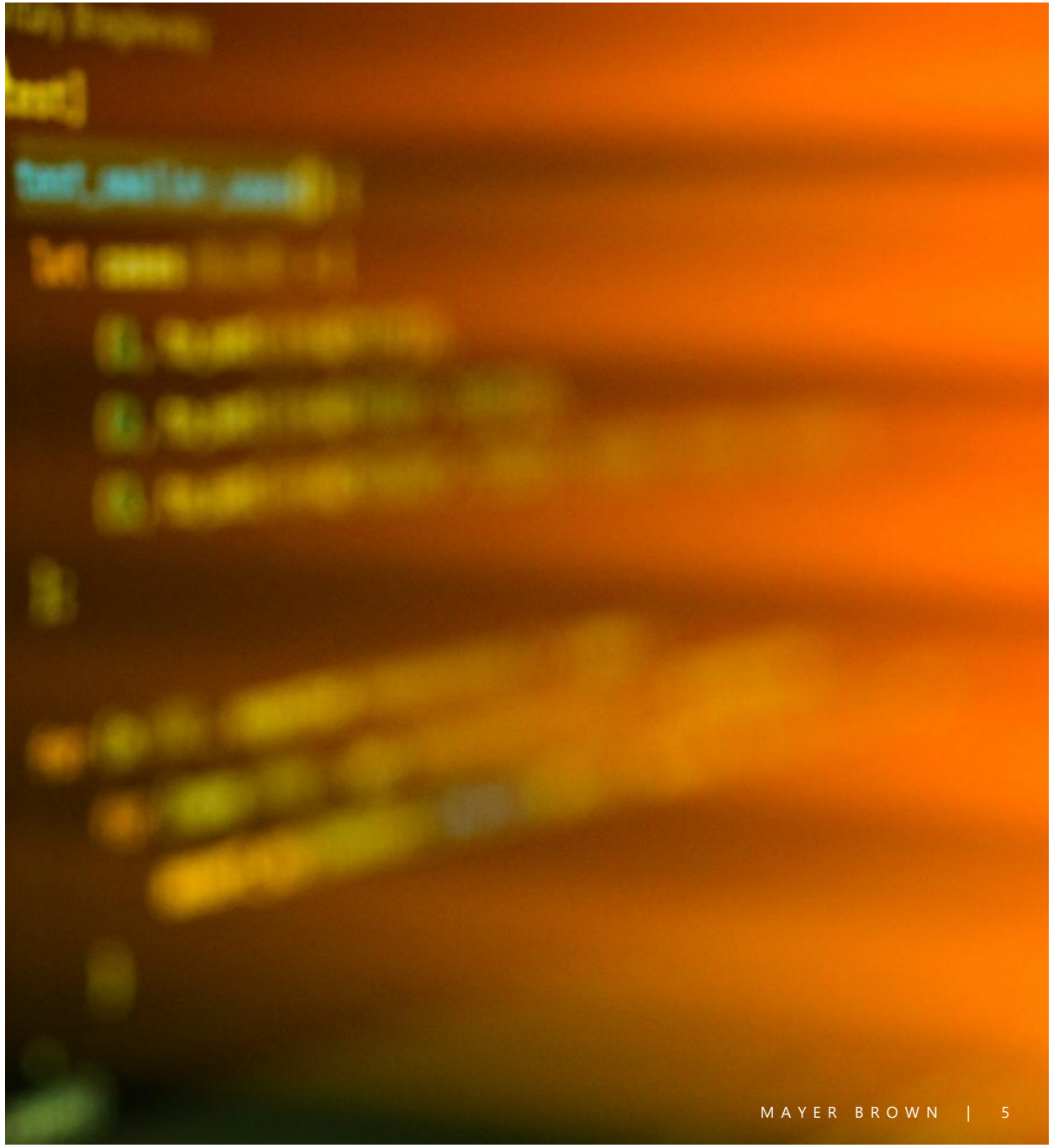


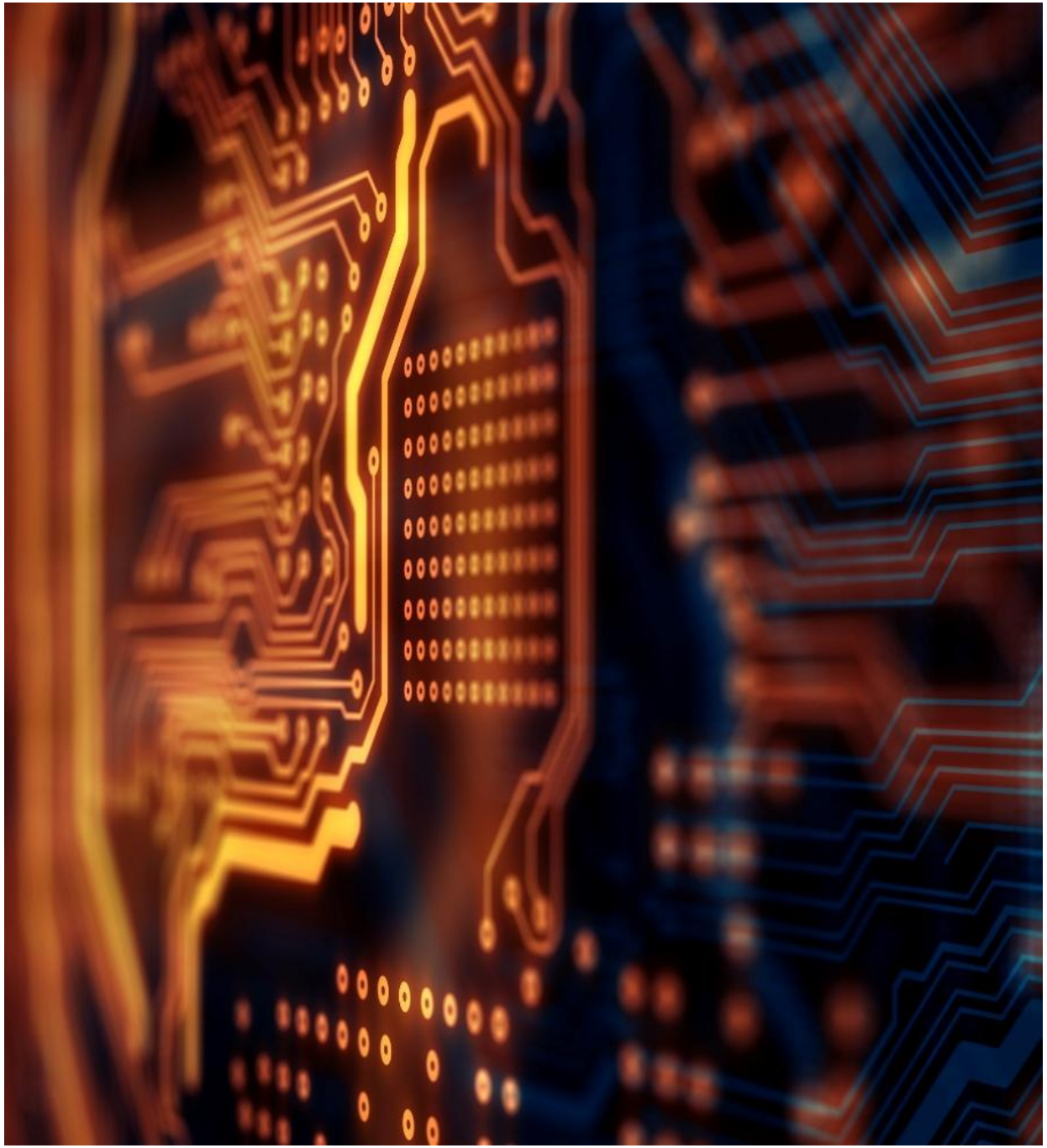
01

OVERVIEW OF THE AUGUST 2026 NSPM

THE NSPM AT A GLANCE

- Signed August 12, 2026: “Expanding Capabilities to Combat Transnational Cyber-Enabled Crime”
- Directs the National Coordination Center (NCC) to create a “Program” of vetted U.S. “Participating Companies”
  - Contract with DOJ or DHS; operate under federal control and oversight
- Targets: foreign Cyber-Enabled Transnational Criminal Organizations (CE-TCOs)
  - Ransomware, phishing, financial fraud, sextortion, impersonation scams
- Not a general “hack back” license — **every operation** needs written government approval and **rests on the government’s authority to conduct the operation**.





TWO CATEGORIES OF OPERATIONS

Cyber Surveillance Operations

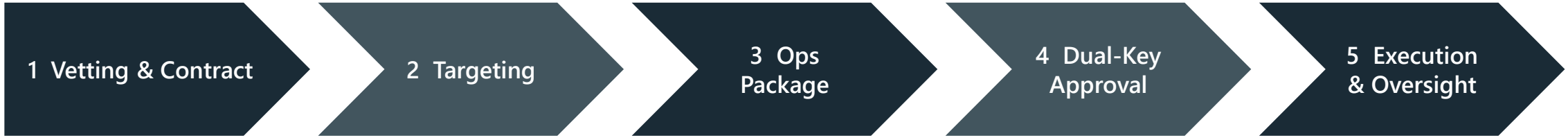
Accessing information systems without the owner's authorization, intending to remain undetected, to collect information or intelligence or to support effects operations.

Cyber Effects Operations

Activity intended to manipulate, disrupt, deny, degrade, or destroy CE-TCO infrastructure.

- Each requires a cyber operations package
- Written approval from DOJ and DHS Executive Directors
- Operational workflow governed by a classified annex

HOW A PROGRAM OPERATION WORKS



Technical, facility, and personnel vetting; contract with DOJ or DHS

Only foreign CE-TCOs; classified adjudicatory framework

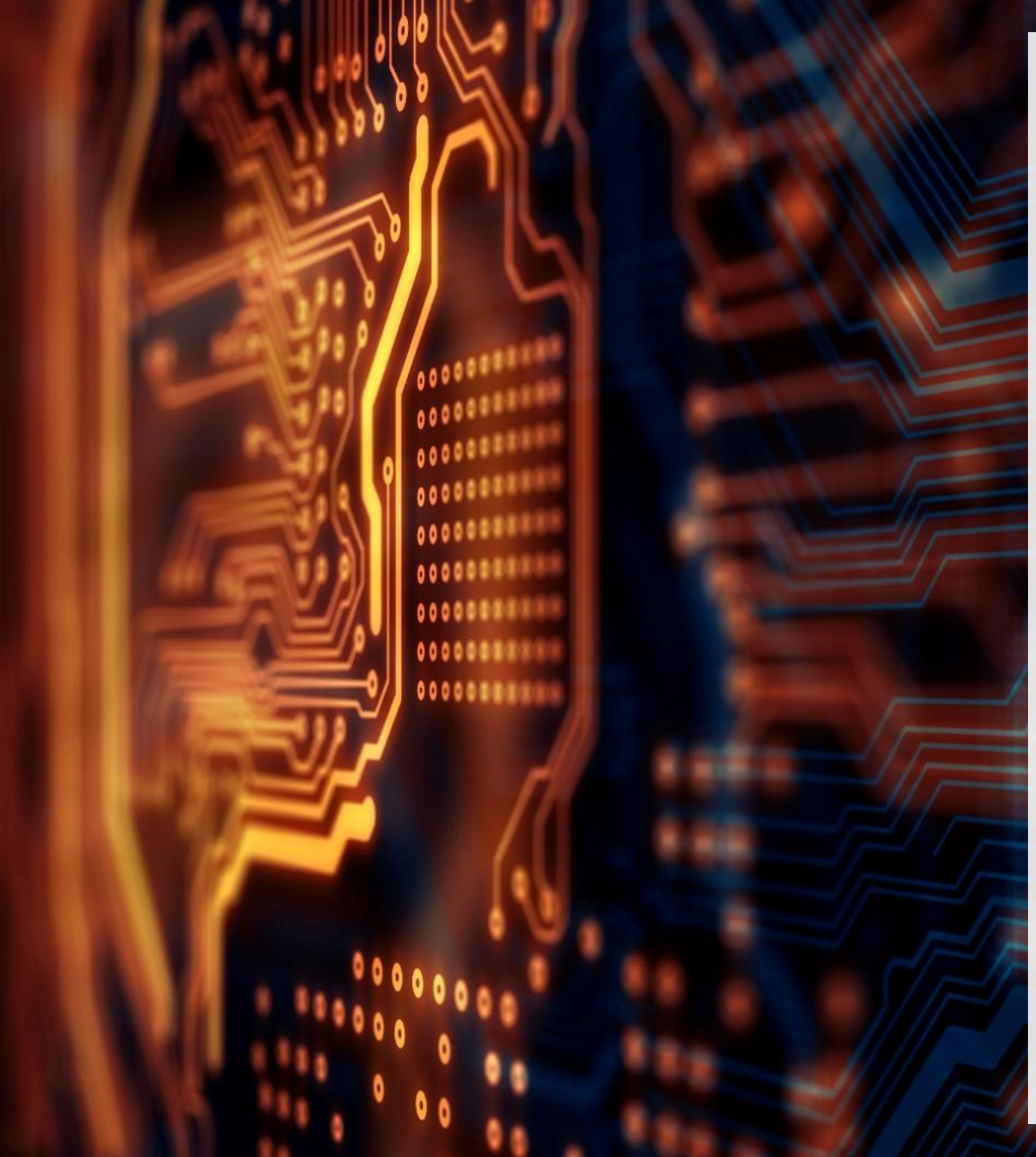
Company submits a proposed surveillance or effects operation

Written sign-off by DOJ and DHS Executive Directors

Conducted under federal direction, control, and reporting

Circuit breakers

Immediately cease, minimize, and notify the NCC (which notifies DOJ) if activity exceeds scope, touches a U.S. person or U.S.-based system, or may produce a Critical Outcome. Participation is reviewed at least annually.



KEY ELEMENTS TO WATCH

Authorities and immunities

How will private actors leverage government authority, e.g., court authorization, delegation of "inherent" authority, or immunity under the law enforcement/intelligence carve-out in 18 U.S.C. § 1030(f)?

Agency roles

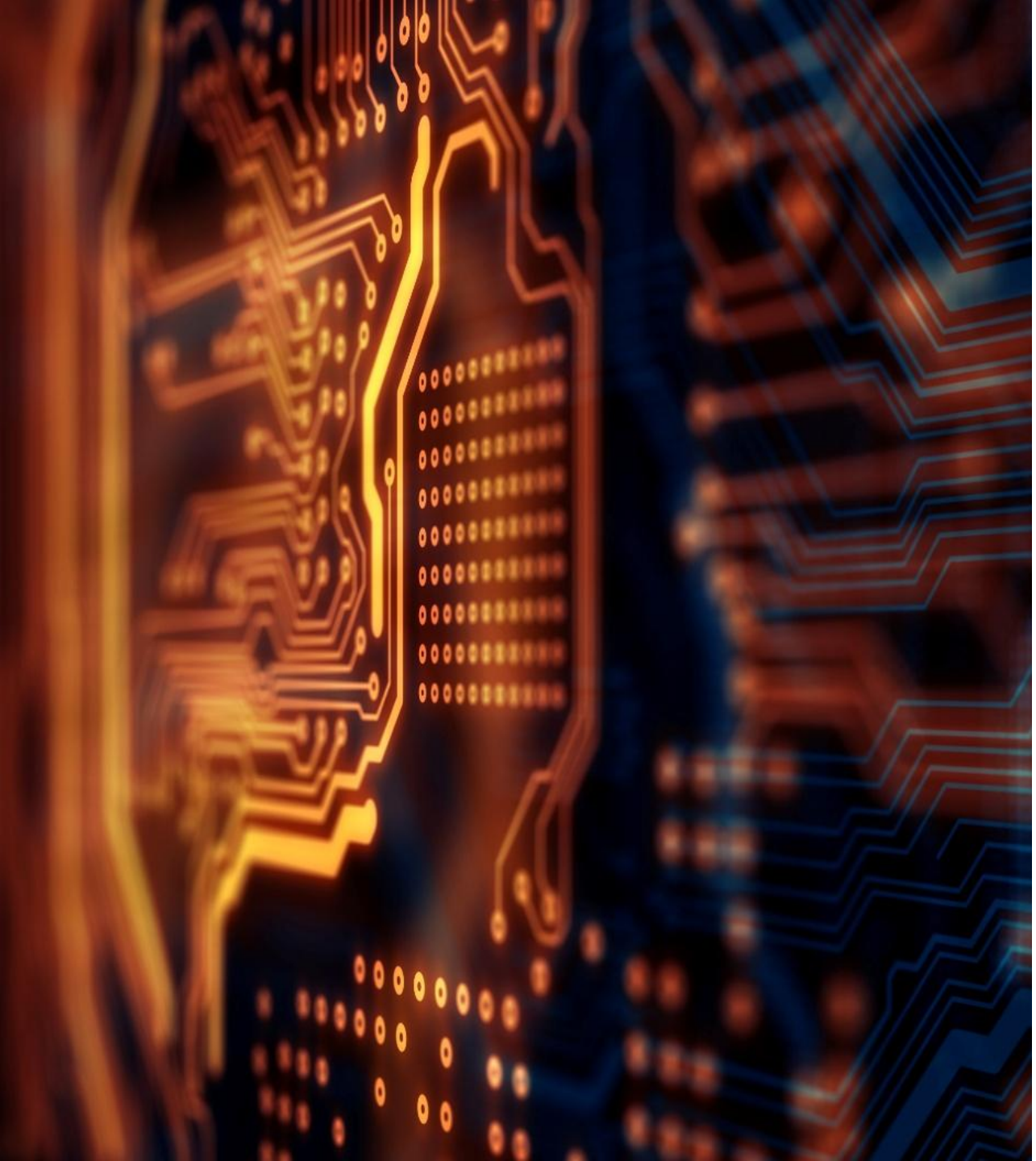
DHS (CISA) as the likely coordinator with industry; DOJ (FBI, CCIPS, NSD) for legal authority and operational control.

- Targets limited to transnational criminal groups
- Deconfliction with government operations
- Liability for collateral consequences



02

HISTORICAL CONTEXT: PPD-20 AND NSPM-13



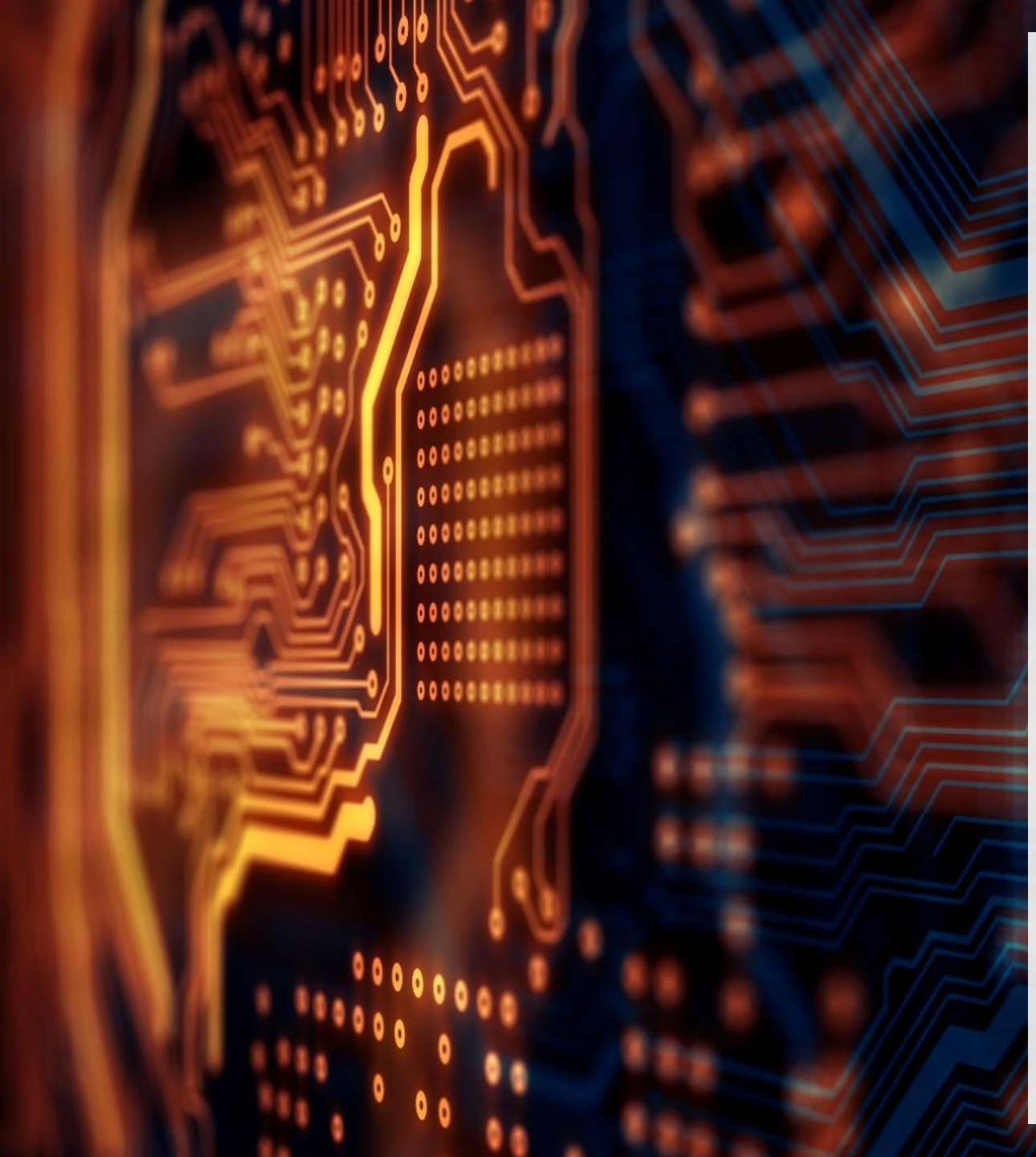
FROM PPD-20 TO NSPM-13

- PPD-20 (Obama, 2012)
  - First U.S. policy formally addressing offensive cyber operations
  - Consensus-driven, NSC-led interagency review; "least action necessary"
  - Classified, but allegedly leaked in 2013 (Snowden)
- NSPM-13 (Trump, August 2018)
  - Replaced PPD-20; delegated authority to the Secretary of Defense for time-sensitive operations
  - Paired with FY2019 NDAA (10 U.S.C. § 394) and "defend forward"
  - Revised in 2022; slated for update under the 2026 Strategy

EVOLUTION OF OFFENSIVE CYBER AUTHORITIES

	PPD-20 (2012)	NSPM-13 (2018)	August 2026 NSPM
Who acts	U.S. government	U.S. government, principally DoD / Cyber Command	Vetted private companies under DOJ/DHS control
Approval model	Interagency consensus via NSC	Delegated to Secretary of Defense for time-sensitive ops	Written per-operation approval by DOJ and DHS Executive Directors
Targets	Foreign threats (national security)	Foreign adversaries; "defend forward"	Foreign CE-TCOs; state actors excluded
Legal anchor	Executive policy (classified)	Title 10 authorities; FY2019 NDAA	Federal law enforcement authority (and CFAA § 1030(f))
Public text	Classified (but reportedly leaked in 2013).	Classified	Public memo with classified annex


03
REGULATORY OVERVIEW



U.S. SURVEILLANCE LAWS

FISA (50 U.S.C. § 1801 et seq.), the Wiretap Act (18 U.S.C. § 2511), the Stored Communications Act, and the Pen/Trap Act limit collecting communications content and metadata (by, variously, private and state-actors).

Relevant exceptions

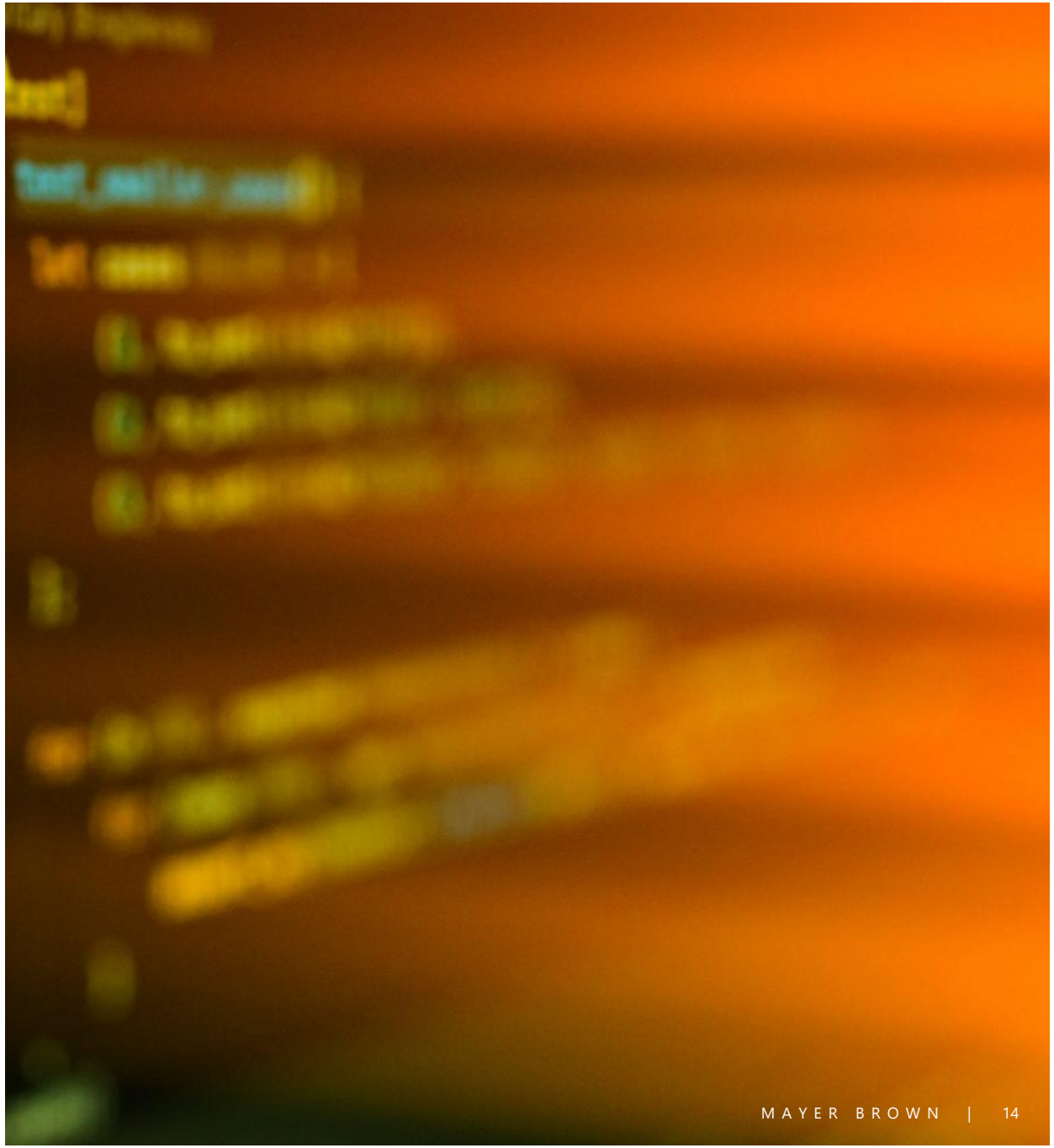
The Wiretap Act "computer trespasser" exception lets owners authorize government interception; it does not authorize private interception.

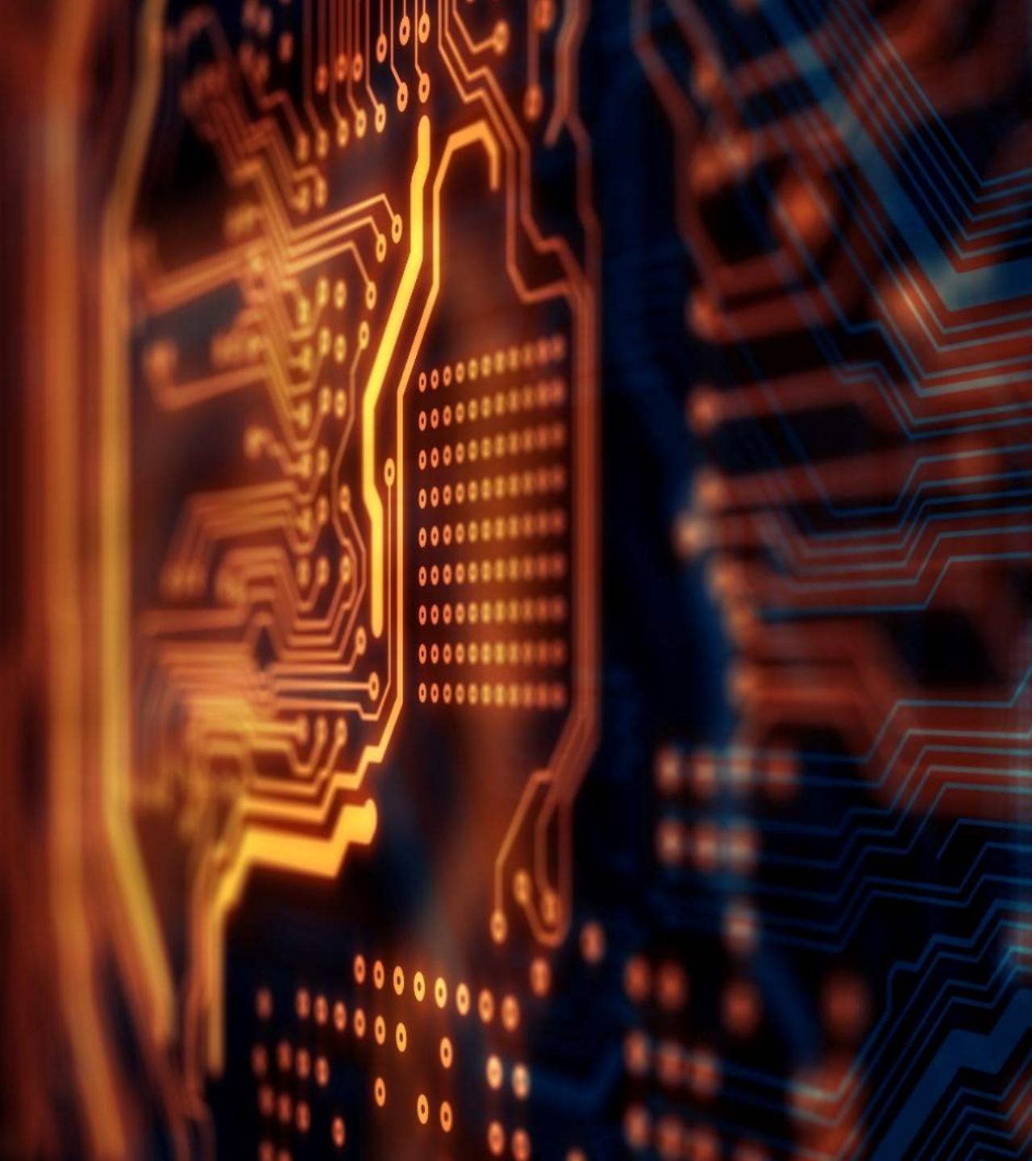
Considerations for all surveillance laws

- Who may collect, what, and under what authority?
- Handling third-party data
- Sharing with government

COMPUTER FRAUD AND ABUSE ACT

- 18 U.S.C. § 1030 prohibits accessing or damaging a computer without authorization, or exceeding authorized access
  - Covers obtaining information, § 1030(a)(2), and causing damage, § 1030(a)(5)
  - "Protected computer" reaches virtually any internet-connected device
  - Civil cause of action under § 1030(g)
- Van Buren v. United States (2021): "gates-up-or-down" approach to authorization
- Applies to activity within or impacting the U.S.
- § 1030(f): does not prohibit lawfully authorized activity of law enforcement or intelligence agencies
  - Potential hook for private actors operating under government authority





DOJ'S LONGSTANDING POSITION

- DOJ (CCIPS) guidance has consistently warned victims not to "hack back"
  - Best Practices for Victim Response and Reporting of Cyber Incidents: do not attempt to access, damage, or impair another network involved in an intrusion
  - Such conduct may violate U.S. and foreign law and can harm innocent third parties
- No self-defense exception in the Computer Fraud and Abuse Act
- 2022 CFAA charging policy: no charges for good-faith security research, but no safe harbor for hack back
- Legislative proposals (e.g., Active Cyber Defense Certainty Act) were introduced but not enacted

ACTIVE DEFENSE VS. HACK BACK

Active defense: your own network

Steps DOJ guidance recognizes

- ✓ Monitor and record activity on your network
- ✓ Reroute traffic; filter or block DDoS attacks
- ✓ Isolate compromised systems
- ✓ Null-route malicious traffic; close ports
- ✓ Contact the admin of the source network
- ✓ Share what you find with law enforcement

Hack back: someone else's system

Off-limits without government authority

- ✗ Access a computer you do not own or operate
- ✗ Modify or damage attacker-linked systems
- ✗ Retrieve data by intruding on another network
- ✗ Retaliate, even against an apparent attacker
- ✗ Rely on informal non-prosecution assurances

Why it matters: hacking back may violate the CFAA and state and foreign law, can hit innocent intermediaries, and can disrupt investigations. The NSPM does not change this for companies acting on their own.

HOW AND WHERE THE RULES APPLY

- Inside your own network: broad latitude (monitoring, deception, honeypots, sinkholing) assuming appropriate consents and other policies.
- Outside your network: CFAA, Wiretap Act, and SCA risk rises sharply
  - Attacker infrastructure is often compromised third-party systems or leased infrastructure
- Cross-border activity: foreign computer misuse and surveillance laws, sovereignty, and diplomatic concerns
- ***Other considerations:***
  - Cybersecurity Information Sharing Act of 2015 "defensive measures" definition
  - sanctions and export controls
  - Contraband information



COURT-AUTHORIZED DISRUPTION

Government-led operations

DOJ has used Rule 41 warrants, forfeiture orders, and pen/trap orders to enable remote, disruption actions. E.g., removing web shells from Exchange servers (2021) and dismantling the Qakbot botnet (2023).

These operations show how oversight, legal process, and transparency come together:

- Court authorization
- Victim notification & public transparency
- Narrowly scoped actions

Private disruption operations

Providers like Microsoft have brought civil actions and obtained TROs authorizing similar relief.

THE CYBER DEFENSE SPECTRUM



Passive Defense

Firewalls, monitoring, logging, patching

Lawful on own network

Active Defense

Null routing, blocking, isolating systems, contacting source admins

Generally lawful if within networks you own or control

Government-Directed Cyber Ops (NSPM)

Companies leverage USG's authorities to conduct operations (and their limitations).

Untested

Offensive Cyber Ops

a/k/a "Hack Back"

Accessing or damaging networks you do not own or control

Likely illegal unless authorized (CFAA, surveillance, civil liability, state & foreign law)



04

CONSIDERATIONS FOR COMPANIES

WHAT THIS MEANS FOR YOUR COMPANY

Considering Participation

Cybersecurity firms weighing a DOJ/DHS contract

1. Run a full legal risk assessment before engaging
2. Do not rely on informal non-prosecution assurances
3. Budget for vetting, the $1M+ bond, and annual review

Vendors, MSSPs & Tool Providers

Supporting operators indirectly

1. Map whether services or tools could support Program operations
2. Assess liability chains from supplying participants
3. Review customer contracts for permitted uses

All Other Companies

Potential victims and data sharers

1. Audit threat-intel sharing, ISAC/ISAO, and vendor clauses
2. Keep honeypots and canary tokens inside the perimeter
3. Plan for retaliatory or collateral activity

NEGOTIATING A PARTICIPATION AGREEMENT

✓ Eligibility & Vetting

NSPM: technical proficiency, proven cyber ops performance, facility security, personnel vetting

✓ Disclosure

NSPM: disclose to the NCC all threat-information agreements with private entities and agencies

✓ Financial Assurance

NSPM: DOJ/DHS may require a bond or escrow of at least $1 million, forfeitable for noncompliance

✓ Indemnification

Coverage and legal representation for litigation arising from approved activities

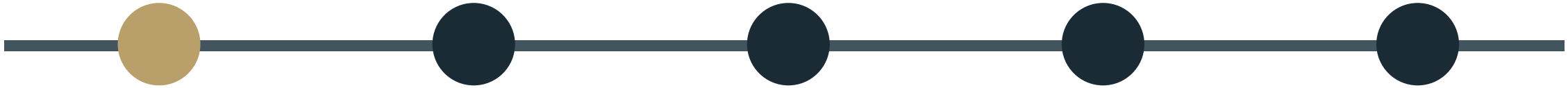
✓ Privilege & Secrecy

Whether the government will invoke state secrets or other privileges

✓ Approval Records

Written approval for every operations package, retained and auditable

WHAT TO WATCH



Now	Next	Feb 2027	Ongoing	TBD
Operating procedures and eligibility standards (due ~mid-October 2026)	Vetting, first DOJ/DHS contracts, and first approved operations	First scheduled status report on the Program to the Assistant to the President and Deputy Chief of Staff for Policy and Homeland Security Advisor and the National Cyber Director	Congress: calls for authorization; parallel SASC contractor provision (June 2026)	First test of the § 1030(f) immunity as applied to private actors.


Q&A
QUESTIONS & DISCUSSION



This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Mayer Brown is a global legal services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England & Wales), Mayer Brown Hong Kong LLP (a Hong Kong limited liability partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively, the "Mayer Brown Practices"). The Mayer Brown Practices are established in various jurisdictions and may be a legal person or a partnership. PK Wong LLC ("PKW") is the constituent Singapore law practice of our licensed joint law venture in Singapore, Mayer Brown PK Wong Pte. Ltd. More information about the individual Mayer Brown Practices and PKW can be found in the Legal Notices section of our website. "Mayer Brown" and the Mayer Brown logo are the trademarks of Mayer Brown. © 2026 Mayer Brown. All rights reserved.