MAYER | BROWN

Virtual Town Hall:
A Conversation on the U.S. Cyber Solarium Commission Report

April 14, 2020

Agenda

- Introduction
- Background & Context for the U.S. Cyberspace Solarium Commission
- Select Commission Recommendations
- Q&A

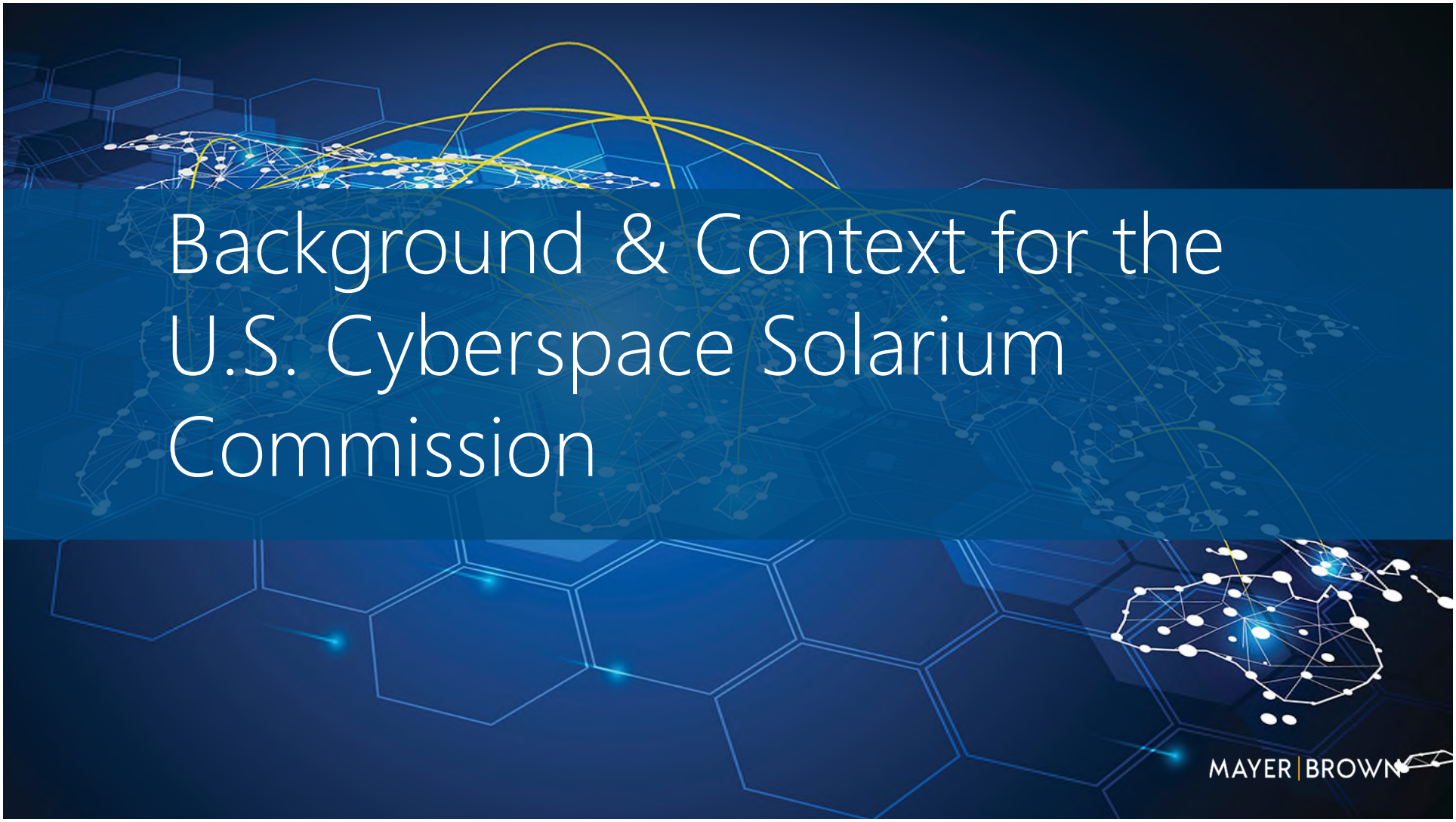

Introduction
MAYER | BROWN

Presenters

David Simon is a partner in Mayer Brown's Washington DC office and a member of the global Cybersecurity & Data Privacy Practice and the firm's National Security Practice. A former special counsel at the U.S. Department of Defense, David has deep experience advising victims of state-sponsored cyber activity, ransomware attacks, and other forms of cyber extortion attacks. He has directed and advised on dozens of complex cybersecurity incident and data breach investigations in the last few years alone. David has counseled companies on major cybersecurity incidents and incident preparedness across virtually every sector of the economy. He advises companies as they address cyber vulnerabilities and breaches, as well as associated legal, regulatory, and reputational consequences. David is currently serving on a pro bono basis as Chief Counsel for Cybersecurity and National Security to the U.S. Cyberspace Solarium Commission.

Suzanne Spaulding is Senior Adviser for Homeland Security at the Center for Strategic and International Studies, where she directs the Defending Democratic Institutions Project. Previously, she served as Under Secretary for the Department of Homeland Security, where she led the National Protection and Programs Directorate, now called the Cybersecurity and Infrastructure Security Agency. Suzanne serves as a Commissioner for the U.S. Cyberspace Solarium Commission.

John C. "Chris" Inglis is a Distinguished Visiting Professor of Cyber Security Studies at the U.S. Naval Academy. He previously served for 28 years at the National Security Agency, including 8 years as its Deputy Director and Senior Civilian Leader. Chris also serves on the U.S. Defense Science Board, where he has participated in or co-led studies on cyber strategy. Chris serves as a Commissioner for the U.S. Cyberspace Solarium Commission.


Background & Context for the U.S. Cyberspace Solarium Commission
MAYER | BROWN

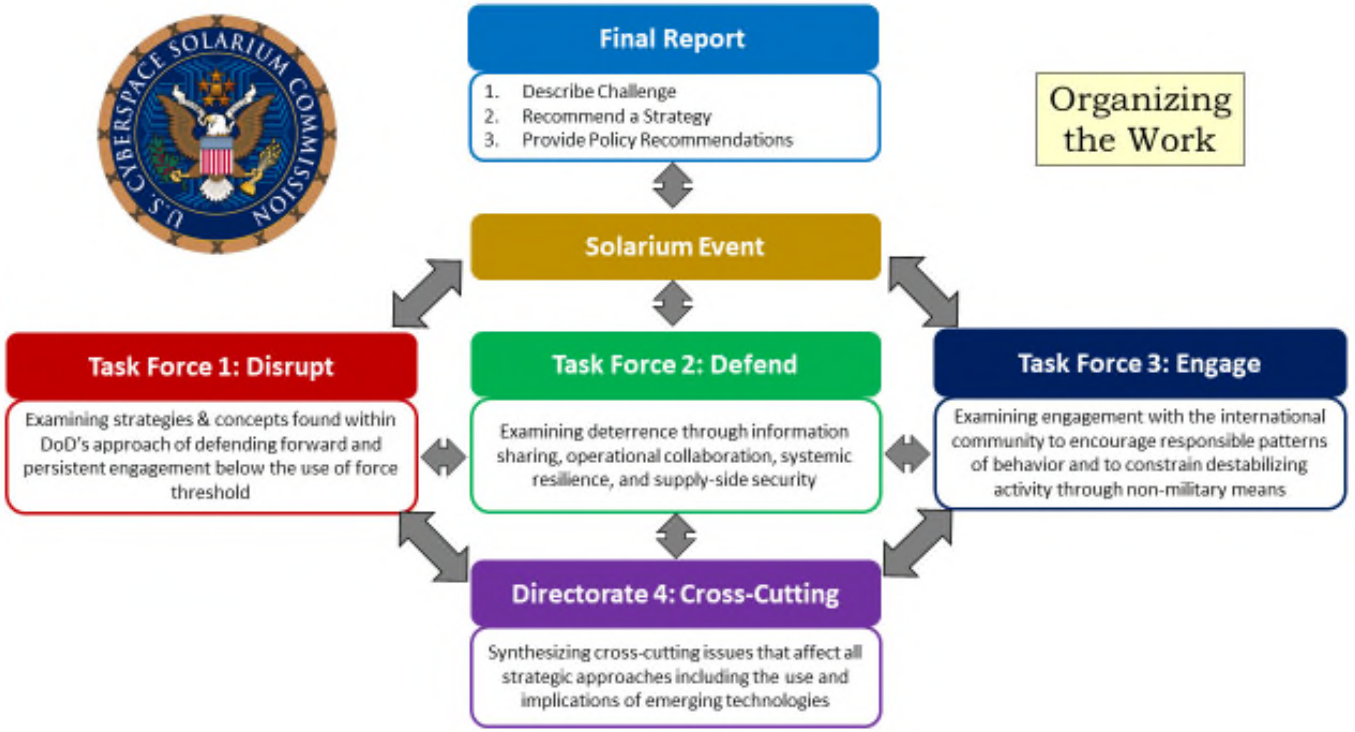
Background

- The **Cyberspace Solarium Commission** (CSC or "the Commission") is inspired by President Eisenhower's Project Solarium. Eisenhower's Solarium developed the strategic approach that would guide the United States through the Cold War.
- Established by the 2019 National Defense Authorization Act, the CSC is a bipartisan, bicameral, intergovernmental, and multisector commission.
- Congress charged the Commission with answering two fundamental questions:
    1. What strategic approach will defend the United States against cyberattacks of significant consequences?
    2. What policies and legislation are required to implement the strategy?

Commissioners

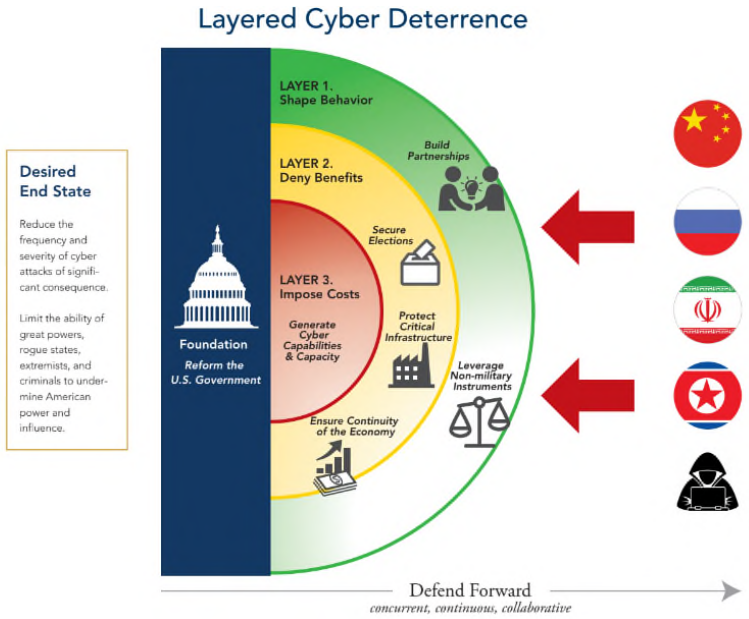
- **Angus S. King, Jr**. – Co-Chairman, CSC, U.S. Senator for Maine
- **Michael "Mike" J. Gallagher** – Co-Chairman, CSC, U.S. Representative for Wisconsin's 8th District
- **Frank Cilluffo** - Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security
- **Thomas A. "Tom" Fanning** - Chairman, President, and Chief Executive Officer of Southern Company
- **Andrew Hallman** - Principal Executive of the Office of the Director of National Intelligence performing the duties of the Principal Deputy Director of National Intelligence
- **John C. "Chris" Inglis** - U.S. Naval Academy Looker Professor for Cyber Security Studies and Former Deputy Director of the National Security Agency
- **James R. "Jim" Langevin** - U.S. Representative for Rhode Island's 2nd District
- **Patrick J. Murphy** - Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District
- **David L. Norquist** - Deputy Secretary of Defense
- **David Pekoske** - Administrator of the Transportation Security Administration & Senior Official Performing the Duties of the Deputy Secretary of Homeland Security
- **Samantha F. Ravich** - Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies
- **Benjamin E. "Ben" Sasse** - U.S. Senator for Nebraska
- **Suzanne E. Spaulding** - Senior Adviser for Homeland Security at the Center for Strategic and International Studies and former Under Secretary for the National Protection and Programs Directorate at the Department of Homeland Security
- **Christopher Wray** - Director of the Federal Bureau of Investigation

Context


Final Report
1. Describe Challenge
2. Recommend a Strategy
3. Provide Policy Recommendations
Organizing the Work
Solarium Event
Task Force 1: Disrupt
Examining strategies & concepts found within DoD's approach of defending forward and persistent engagement below the use of force threshold
Task Force 2: Defend
Examining deterrence through information sharing, operational collaboration, systemic resilience, and supply-side security
Task Force 3: Engage
Examining engagement with the international community to encourage responsible patterns of behavior and to constrain destabilizing activity through non-military means
Directorate 4: Cross-Cutting
Synthesizing cross-cutting issues that affect all strategic approaches including the use and implications of emerging technologies

Development Process & Structure

- Conducted an extensive study including over 300 interviews, red teaming, tabletop, research staff, etc.
- Commission advocates a new strategic approach to cybersecurity: **layered cyber deterrence**



MAYER | BROWN


Select Commission
Recommendations
MAYER | BROWN

Recommendations

75 Recommendations under 6 Pillars

- Reshape the cyber ecosystem toward greater security (Pillar 4)
- Promote national resilience (Pillar 3)
- Operationalize cybersecurity collaboration with the private sector (Pillar 5)
- Reform government structure (Pillar 1)
- Strengthen norms and non-military tools (Pillar 2)
- Preserve and employ the military instrument of power (Pillar 6)

Note: *Forty-nine of the recommendations have corresponding draft* ***legislative proposals***.


Reshape the Cyber Ecosystem Toward Greater Security (Pillar 4)
MAYER | BROWN

Rec. 4.2 — Establish Liability for Final Goods Assemblers

Context:

- There are no generally applicable legal or regulatory requirements specific to software patching. Software vendors define their own standard of reasonableness.

Content:

- "Congress should **enact legislation establishing that final goods assemblers of software, hardware, and firmware are liable for damages from incidents that exploit vulnerabilities** that were known at the time of shipment or discovered and not fixed within a reasonable amount of time."
- Congress should direct the FTC to mandate transparency from final goods assemblers.

Rec. 4.3 — Establish a Bureau of Cyber Statistics

Context:

- Agencies like the Bureau of Labor Statistics establish the metrics and reporting by which government policy and private-sector efforts are measured. The United States has no national equivalent for national cybersecurity.

Content:

- "Congress should **establish a Bureau of Cyber Statistics** within the Department of Commerce, or another department or agency, that would act as the government statistical agency that **collects, processes, analyzes, and disseminates essential statistical data on cybersecurity, cyber incidents, and the cyber ecosystem** to the American public, Congress, other federal agencies, state and local governments, and the private sector."
- The Bureau would focus on issues ranging from **cyber incident reporting**, to **conducting data surveys**, as well as defining and promulgating **cyber security metrics** for the private sector.

Rec. 4.4.4 — Amend Sarbanes-Oxley Act for Cybersecurity

Context:

- Cybersecurity of publicly traded companies is a critical component of financial and business risk. The **Sarbanes-Oxley Act** imposes certain reporting requirements to the SEC to demonstrate financial health. The Act currently does not account for cybersecurity.

Content:

- Congress should amend the Sarbanes-Oxley Act to explicitly account for cybersecurity.
  - Include a definition of an "information system."
  - Specify corporate responsibility requirements for the security of information systems, including those for risk assessments, determinations, decisions, cyber hygiene, penetration testing and red-teaming results.
  - Mandate that public companies maintain internal records of cyber risk assessments to allow for a full evaluation of cyber risks in M&A or legal/regulatory action.
  - "Require management assessments and attestations of plans to manage risk from information systems and data."

Rec. 4.7 — Pass a National Data Security & Privacy Protection Law

Context:

- Competing state legal and international frameworks threaten to splinter the digital economy and confuse efforts to secure users' personal data.

Content:

- "Congress should **pass legislation standardizing requirements** that are enduring for the safe and appropriate handling of personal data." This should include:
  - "National minimum common standards for the collection, retention, analysis, and third-party sharing of personal data.
  - Definitions of personal data, to include that which can be linked, directly or indirectly, to individuals or households.
  - Thresholds for what entities are covered by this legislation.
  - Timelines for deleting, correcting, or porting personal data upon request by the appropriate persons.
  - A clear mandate for the Federal Trade Commission to enforce these standards with civil penalties."

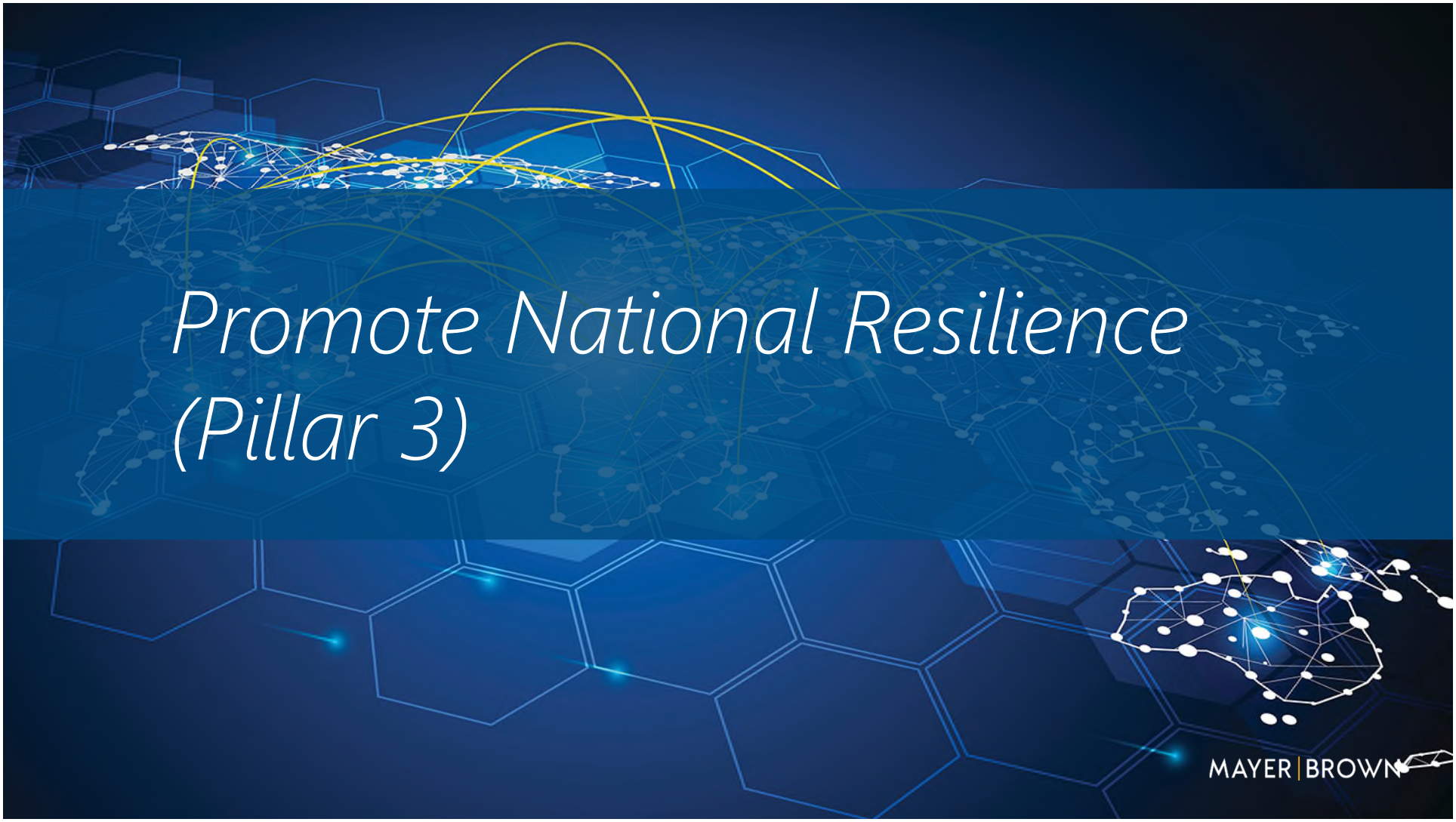
Rec. 4.7.1 — Pass a National Data Breach Notification Law

Context:

- Companies face a patchwork of 50 state laws governing data breach requirements that create significant compliance challenges in an area where uniformity has the potential to benefit consumers and companies.

Content:

- "Congress should pass a national breach notification law that:
  - Preempts the 54 existing state, district, and territorial data breach notification laws.
  - Establishes a threshold for what would be considered a covered 'breach.'
  - Requires the notification and transmission of relevant forensic data to the appropriate law enforcement and cybersecurity authorities and other relevant anonymized data to authorized data-gathering bodies, such as the Bureau of Cyber Statistics proposed in recommendation 4.3 . . .
  - Sets standards and timelines for notifying victims.
  - Sets criteria that determine when victims should receive free credit monitoring or other data and identity protections.
  - Deconflicts with existing federal regulation for private-sector and other non-federal entities."


Promote National Resilience
(Pillar 3)
MAYER | BROWN

Rec. 3.2 — Develop & Maintain Continuity of the Economy Planning

Context:

- **Continuity of Operations** and **Continuity of Government** have long been cornerstones of government contingency planning, but no equivalent effort exists to ensure the rapid restart and recovery of the U.S. economy after a major cyber disruption.

Content:

- "Congress should direct the executive branch to **develop and maintain Continuity of the Economy** planning in consultation with the private sector to ensure the continuous operation of critical functions of the economy in the event of a significant cyber disruption."
- The planning should focus on efforts to maintain the continuity of distribution or commerce, as long-term disruptions to key sectors of the economy could undermine the United States' "international standing, credibility, and appeal" in the global marketplace.

Rec. 3.3 — Codify a "Cyber State of Distress"

Context:

- **Presidential Policy Directive 41** and the **National Cyber Incident Response Plan** do not empower federal agencies with additional FEMA-like authorities to respond to a "significant cyber incident."

Content:

- Congress should pass a law **codifying a** "**Cyber State of Distress**"—a federal declaration that would trigger the availability of additional resources through a "**Cyber Response and Recovery Fund**"—to assist the private sector.
- The law would cover preemptive action and preparation, where the federal government has "a reasonable expectation that a significant cyber incident is likely to occur and preemptive action and preparation would reduce potential consequences of disruption or compromise."

Rec. 3.5 — Build Societal Resilience to Foreign Malign Cyber-Enabled Information Operations

Context:

- "Cyber-enabled information operations endanger our national security by threatening to undermine trust and confidence in American democracy and its institutions—including but also extending beyond our elections. Americans must become better equipped to recognize such operations, so that they can mitigate their damage in the future."

Content:

- The U.S. government should **promote digital literacy, civics education, and public awareness** to build societal resilience to foreign malign cyber-enabled information operations.
- "Congress should (1) direct the Government Accountability Office (GAO) to evaluate the effectiveness of government spending on cybersecurity awareness efforts"; and "(2) authorize and fund DHS . . . to establish a grant program seeking research and proposals for effective mechanisms to improve, develop, and implement a public awareness and education initiative on cybersecurity."


Operationalize Cybersecurity Collaboration
with the Private Sector (Pillar 5)
MAYER | BROWN

Rec. 5.1 — Codify the Concept of "Systemically Important Critical Infrastructure"

Context:

- "**Systemically Important Critical Infrastructure**" (SICI) entities are often targeted by nation-state adversaries, posing an incredible risk to the United States.

Content:

- Congress should **codify the concept of SICIs**, providing such entities with U.S. government support and requiring these entities to adhere to additional security requirements.
- These entities are still ultimately responsible for the defense and security of their networks, but the U.S. government should leverage its "unique authorities, resources, and intelligence capabilities to support these entities in their defense."

Rec. 5.1.3 —Administrative Subpoenas for Threat and Asset Response

Context:

- U.S. law enforcement and regulatory agencies face significant challenges consistently identify victims of vulnerable or compromised online systems, preventing the federal government from effectively notifying and assisting private-sector entities with their data security/cybersecurity operations.

Content:

- "Congress should consider granting certain departments and agencies subpoena authority in support of their threat and asset response activities, while ensuring appropriate liability protections for cooperating private-sector network owners." There are two ways in which this may occur:
  - Extend existing law enforcement administrative subpoena authority for the FBI and Secret Service to include violations of the Computer Fraud and Abuse Act.
  - Pass the **Cybersecurity Vulnerability Identification and Notification Act of 2019**, which grants certain additional powers to the Director of the Cybersecurity and Infrastructure Security Agency (CISA) to serve administrative subpoenas to identify owners of online systems with known vulnerabilities.

Rec. 5.2.2 — Pass National Cyber Incident Reporting Law

Context:

- It is currently difficult to quantify the state of private sector cybersecurity and preparedness due to inconsistent and incomplete reporting of cybersecurity intrusions to the federal government.

Content:

- "Congress should authorize DHS and [DOJ] to establish requirements for **critical infrastructure** entities to report cyber incidents to the federal government."
- DHS and DOJ would collaborate with public- and private-sector entities to identify the different categories of critical infrastructure entities that should be covered under the law.


Reform the U.S. Government's Structure
and Organization for Cyberspace (Pillar 1)
MAYER | BROWN

Rec. 1.2 — House/Senate Committees on Cybersecurity

Context:

- Legislative and budgetary jurisdiction, as well as oversight, for cybersecurity is dispersed across multiple committees and subcommittees in both chambers of Congress.
- In addressing abuses of authority in the Intelligence Community, Congress established specific committees in both house focused exclusively on intelligence issues and oversight.

Content:

- Congress should **establish a House Permanent Select Committee and a Senate Select Committee on Cybersecurity** modeled off those House and Senate committees governing national intelligence (HPSCI/SSCI).
- These committees would have legislative jurisdiction both within government and over relations between the government and private sector.

Rec. 1.3 — Establish a National Cyber Director

Context:

- The executive branch lacks a streamlined approach to address responsibilities and authorities over cyberspace. Many departments and agencies seek similar resources and roles sometimes overlap power, resulting in conflicting or overlapping efforts.

Content:

- Congress should **establish a National Cyber Director** (NCD), within the Executive Office of the President, who is Senate-confirmed and supported by the Office of the National Cyber Director.
- "The NCD would serve as the President's principal advisor for cybersecurity and associated emerging technology issues; the lead for national-level coordination for cyber strategy, policy, and defensive cyber operations; and the chief U.S. representative and spokesperson on cybersecurity issues."


Strengthen Norms and Non-Military Tools
(Pillar 2)
MAYER | BROWN

Rec. 2.1 — Create a Cyber Bureau at U.S. State Department

Context:

- The United States needs a more forward leaning posture in the development of international and multilateral cyber norms, as well as bilateral cyber cooperation and intelligence sharing agreements.

Content:

- "Congress should **create the Bureau of Cyberspace Security and Emerging Technologies** (CSET), led by an Assistant Secretary reporting to the Under Secretary for Political Affairs, or someone of higher rank."

Rec. 2.1.4 — Improve Int'l Tools for Law Enforcement

Context:

- Law enforcement tools like criminal indictments and international extraditions are important parts of cyber deterrence.

Content:

- "Improve the MLAT/MLAA Process: **Mutual Legal Assistance Treaties** (MLATs) and **Mutual Legal Assistance Agreements** (MLAAs) are tools that enable U.S. law enforcement to prosecute cybercriminals." DOJ's Office of International Affairs should have administrative subpoena authority and "Congress should provide funding to the FBI to help automate the execution of MLAT/MLAA-related search warrants."
- "Increase the Number of FBI Cyber ALATs: Congress should create and fund 12 additional **FBI Cyber Assistant Legal Attachés** (ALATs) to facilitate intelligence sharing and help coordinate joint cyber operations."

Rec. 2.1.5 — Leverage Sanctions & Trade Enforcement

Context:

- The United States should join the international community in strengthening its dedication to using economic sanctions against those who conduct cyberattacks on the U.S. electoral process and infrastructure.

Content:

- "Congress should codify into law Executive Order 13848, '**Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election**.'"
- "The Office of the United States Trade Representative should consider taking action under **Section 301 of the Trade Act of 1974**, and the Department of Commerce should consider using the **Entity List**—part of the Export Administration Regulations—to impose further requirements."


Preserve and Employ the Military Instrument of Power (Pillar 6)
MAYER | BROWN

Rec. 6.2.1 — Require Defense Industrial Base Participation in a Threat Intelligence Sharing Program

Context:

- The **Defense Industrial Base** needs to develop a common understanding of the threat environment applicable to their sector and facilitate increased support by their federal government partners.

Content:

- "Congress should legislatively require companies that make up the Defense Industrial Base, as part of the terms of their contract with DoD, to participate in a threat intelligence sharing program that would be housed at the DoD component level."

Rec. 6.2.2 — Require Threat Hunting on Defense Industrial Base Networks

Context:

- The **Defense Industrial Base** needs to improve the way in which threats are detected and mitigated.

Content:

- "Congress should . . . direct regulatory action that the executive branch should pursue in order to require companies that make up the Defense Industrial Base, as part of the terms of their contract with DoD, to create a mechanism for **mandatory threat hunting on DIB networks**."


Q&A
MAYER | BROWN

Americas | Asia | Europe | Middle East

mayerbrown.com