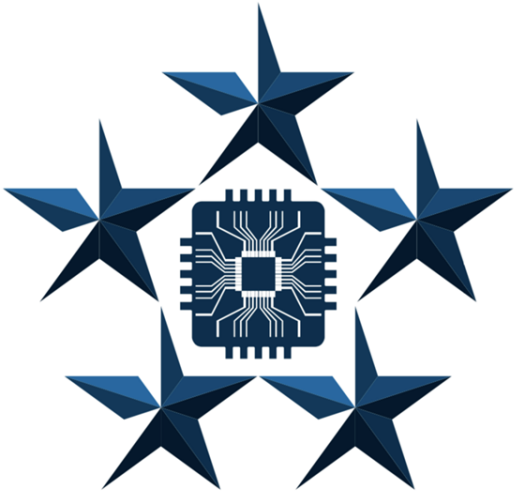


UNITED STATES OF AMERICA

CYBERSPACE SOLARIUM COMMISSION

Water ISAC

July 1, 2020

Bottom Line Upfront

- Cyberspace Solarium Commission created by law (NDAA 2019) to recommend a strategic approach to protect the United States against a cyber incident of significant consequence
    - 14 Commissioners – 4 serving legislators; 4 executive branch leaders; and 6 appointed members (business, academia, think tank, former government….)
    - Focused on a new "strategic approach" and the policy/legislative remedies to implement that approach
- Final report issued on 11 March 2020
    - www.solarium.gov
    - Strategy and 80 + recommendations (more than 50% have legislative component)

Deterrence is not Working Across all of Cyberspace

Escalating Nation-State and Criminal Cyber Attacks on Public and Private Sectors

- Massive Intellectual Property Theft from U.S. 2008 – 2016
- Denial of Service Attacks on U.S. Financial Infrastructure, 2012 - 2013
- Disruption and Theft against Sony Pictures, 2014
- Theft of U.S. Office of Personnel Management Security Records, 2015
- Interference in U.S. National Elections, 2016
- *Wannacry* Global Ransomware, April 2017
- *NotPetya*, Massive Disruption and Destruction, June 2017
- Attempted interference in U.S. National Elections, 2018
- Growing trend of unchecked ransomware attacks, 2019

"Significant" Threats involve Theft, Disruption, Destruction and Subversion

Cyberspace Solarium Commission

An Opportunity to Reconsider and Recast

The John S. McCain National Defense Authorization Act of FY 2019

Mission: "Develop a strategic approach to defending the United States in cyberspace against cyber-attacks of <u>significant</u> consequences."

<u>Study a number of strategic options:</u>

- Active disruption of adversary attacks (Task Force 1)
- Deterrence (Task Force 2)
- Norms-based regimes (Task Force 3)

STATUS UPDATE

300+ STAFF ENGAGEMENTS

30 + COMMISSION MEETINGS

UNITED STATES OF AMERICA
CYBERSPACE SOLARIUM COMMISSION

MANDATE

Section 1652 of the Fiscal Year 2019 National Defense Authorization Act (NDAA) established the Cyberspace Solarium Commission as an independent Commission to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences."

COMMISSIONERS

4 LEGISLATIVE BRANCH

Sen. Angus King
I-ME
(Co-Chair)

Rep. Michael Gallagher
R-WI
(Co-Chair)

Sen. Ben Sasse
R-NE

Rep. Jim Langevin
D-RI

4 EXECUTIVE BRANCH

Andrew Hallman
Fmr. ODNI

David Norquist
DOD

David Pekoske
DHS

Chris Wray
FBI

6 ACADEMIA, THINK TANKS, PRIVATE SECTOR

Frank Cilluffo
Auburn University

Chris Inglis
U.S. Naval Academy

Suzanne Spaulding
CSIS

Samantha Ravich
Foundation for Defense of Democracies

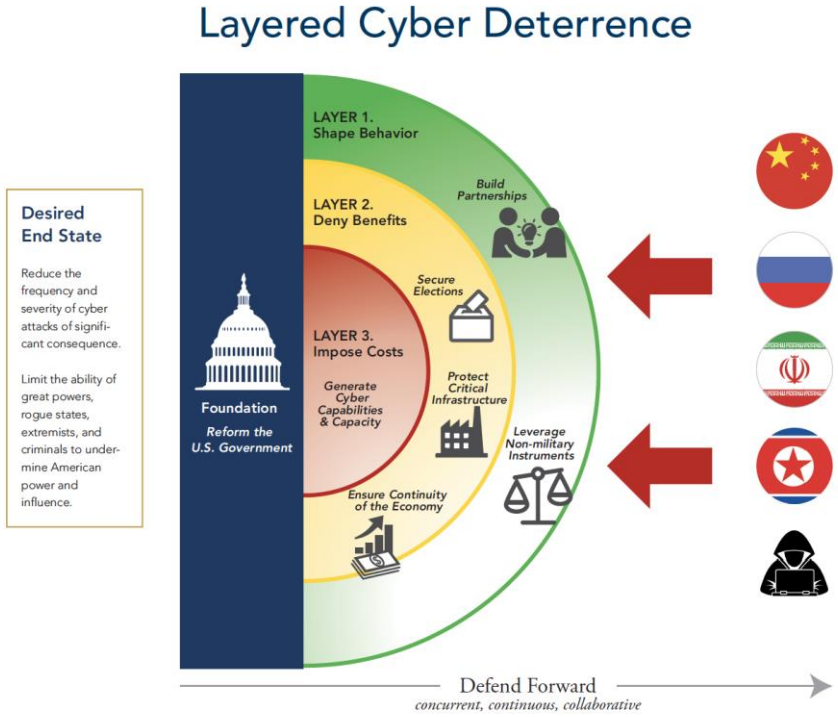
Tom Fanning
Southern Company

Hon. Patrick Murphy
Fmr. Undersecretary, U.S. Army
Fmr. U.S. Representative (D-PA)

DATES

- **INITIAL MEETING**
  APRIL 2019
- **SOLARIUM EVENT**
  OCTOBER 2019
- **FINAL REPORT ISSUED**
  11 MARCH 2020

A New Strategic Approach to Cybersecurity for the Nation



The Implementation:

Pillar 1 - Reform the U.S. Government's Structure and Organization for Cyberspace;

Pillar 2 - Strengthen Norms and Non-Military Tools;

Pillar 3 - Promote National Resilience;

Pillar 4 - Reshape the Cyber Ecosystem towards Greater Security;

Pillar 5 - Operationalize Cybersecurity Collaboration with the Private Sector;

Pillar 6 - Preserve and Employ the Military Instrument of Power - and All Other Options to Deter Cyber-attacks at Any Level.

Emergent Conclusions

- **Deterrence is <u>not</u> working** to stop our adversaries' actions in the grey zone, short of armed conflict.
- **Deterrence <u>can</u> work.**
  - But it will differ from cold war model.
- **Public-Private partnership is crucial** in cybersecurity.
  - Where the vast majority of cyberspace and our critical infrastructure is owned and operated by the private sector.
- **Defense and resilience is a meaningful differentiator** in cyberspace.
  - And for years, we have been delinquent in investing in meaningful defense and resilience.

Key Recommendations for the Water Sector

1. Resourcing and codifying the responsibilities of the **sector-specific agencies** that manage day-to-day engagement with the private sector.
2. Establishing a five-year **national risk management cycle** and **critical infrastructure resilience strategy** tied to a **National Cybersecurity Assistance Fund** to provide consistent, institutionalized funding for projects that mitigate national risk.
3. Developing a **continuity of the economy (COTE)** plan to ensure the continuous operation of critical functions of the economy in the event of a significant cyber disruption.
4. Codifying a new social contract between government and **systemically important critical infrastructure (SICI)** to recognize the unique resources, roles, and responsibilities that are necessary to protect critical systems and assets.
5. Providing more transparent and understandable information on the security of IT and OT goods and services through the creation of a non-governmental **National Cybersecurity Certification and Labeling Authority.**