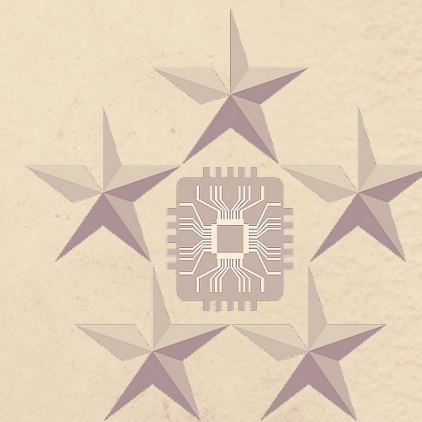




PRESERVING THE LEGACY AND CONTINUING THE WORK OF THE CYBERSPACE SOLARIUM COMMISSION (CSC): THE CSC 2.0 PROJECT

1

Philip Niedermair



CSC 2.0

"NEVER IN THE FIELD
OF HUMAN CONFLICT
HAS SO MUCH BEEN
OWED BY SO MANY TO
SO FEW"

- Winston Churchill

"NEVER IN THE FIELD
OF HUMAN CONFLICT
HAS SO MUCH
RESPONSIBILITY BEEN
GIVEN BY SO MANY TO
SO FEW"

THE US CYBERSPACE SOLARIUM COMMISSION READING ON CAPITOL HILL



Six Pillars of The US Cyberspace Solarium Commission Strategy

1. Reform the US government structure & organization for Cyberspace
2. Strengthen norms in non-military tools so that we can compete and defend ourselves effectively
3. Promote national resilience across all components of our infrastructure and economy.
4. Reshape the cyber ecosystem toward greater security.
5. Operationalize cyber security collaboration within the private sector.
6. Preserve and employ the military as an instrument of power and all other options that can be used to deter cyber attacks at any level so that our mission is clear to defend our nation from cyber attacks from both independent actors and nation-states

The US Cyberspace Solarium Commission Additional Recommendations

In addition, the Commission issued six position papers with new and updated recommendations. They addressed lessons on cybersecurity from the pandemic, details on the recommendation to establish the Office of the National Cyber Director (ONCD), a framework for a cybersecurity workforce development strategy, proposals on how to secure America's information and communications technology (ICT) supply chains, and recommendations to counter malign foreign disinformation.

CSC 2.0 Year 2 Assessment

Original 82 recommendations stats for 2021

- Roughly 35% were fully implemented or nearing implementation
 - Nearly 45% were on track

Original 82 recommendations stats for 2022

- Nearly 60% are fully implemented or nearing implementation
- More than 25% are on track to implementation

CSC 2.0 Year 2 Assessment

When you include Position Papers – its 116 recs – and Similar completion rates
(60% / 25%)

Authorizing Legislation:

- FY21 NDAA: 27 provisions that implement 25 different CSC recommendations
- FY22 NDAA: includes additional 12 recommendations
- Infrastructure Investment & Jobs Act: 6 recommendations
- CHIPS and Science Act: 11 recommendations

8

Appropriations:

- FY21 appropriations: 19 funding priorities
- FY22 appropriations: 42 funding priorities
- FY23 appropriations: 35 funding priorities

Continuing the Legacy of the US Cyberspace Solarium Commission (CSC): The Work Plan for the CSC 2.0 Project

The CSC 2.0 project will preserve the legacy of the Cyberspace Solarium Commission and continue the work to implement its recommendations. Specifically, the project will:

- Conduct and publish an Annual Assessment of legislative/executive progress on CSC recommendations
- Conduct research and analysis related to outstanding CSC legislative recommendations
- Provide research to policymakers as they implement executive branch CSC recommendations
- Represent CSC positions/policy recommendations at conferences, panels, hearings

Continuing the Legacy of the Cyberspace Solarium Commission (CSC): The Work Plan for the CSC 2.0 Project

The project will conduct research and analysis and develop policy proposals in five issue areas:

- Cybersecurity in the Water/Wastewater Sector
- Federal Cybersecurity Workforce Development
- Continuity of the Economy Planning
- Cybersecurity in the Maritime Transport System Sector
- Cybersecurity in the Healthcare Sector

You can engage and hopefully gain access to useful data and content from us at www.cybersolarium.org

CSC 2.0 Summary: Education Initiative

Improve Cyber-Oriented Education. The Federal Government should:

- Develop a secure online clearinghouse for K-12 cybersecurity resources
- Develop work-based learning programs and apprenticeships
- Support cybersecurity clinics at colleges and universities
- Expand the existing Centers of Academic Excellence program
- Incorporate cybersecurity into safety curricula for career & technical programs
- Promote professional development programs for K-12 teachers
- Explore ways to expand programs such as the FBI Cyber STEM program and CISA's Cybersecurity Education Training Assistance Program

CSC 2.0 Important Work to Be Accomplished

Time to Designate Space Systems as Critical Infrastructure

The Criticality of Space Systems and Threats to the Sector Space systems serve fundamental roles in national security and economic prosperity and are at risk of disruption.

These risks stem from adversarial nations intent on causing harm to the United States and its partners and allies and are amplified by legacy technologies and the unique challenges of space. Currently, space systems serve as the foundation for:

- Military operations, mission assurance, and intelligence, surveillance, and reconnaissance.
- Critical infrastructure sectors — energy and water, for example — rely heavily on satellites for positioning, navigation, and timing for industrial control systems that power pipelines and transmission lines.
- Within the financial services sector, trading and transactions, ATMs, and credit cards all rely on space systems
 - As do the telecommunications, maritime transportation, and agricultural sectors.

CSC 2.0 Important Work to Be Accomplished

In daily life, Americans rely on the global positioning system (GPS). Meanwhile, the economic impact of space systems is growing rapidly, prompting at least one expert to suggest the economic dimension may soon equal and surpass the national security impact.

Estimates project within 10 to 15 years, the value of the space industry could approach \$1 trillion worldwide. The Department of Commerce estimates that in 2019, the U.S. space economy generated \$194.4 billion in real gross output — an increase of 20 percent from earlier in the decade, translating to 0.6 percent of U.S. gross domestic product.¹² During fiscal year 2021, NASA alone “generated a total economic output of more than \$71.2 billion,”

13

Alongside these developments, soon-to-be-operational, fully reusable space launch systems made by SpaceX, Blue Origin, and others will have a transformative impact on space logistics and national defense.¹⁴ America’s adversaries recognize the importance of space systems to U.S. national and economic security and have tested capabilities to destroy them.

The Time to Designate Space Systems as Critical Infrastructure is NOW

Ongoing Indirect Impact of the US Cyberspace Commission & CSC 2.0

Across the nation and in the camps of our allies- CYBER STRATEGY is becoming more unified - Not necessarily because of our report, but notably recently, we have seen innovative and significant action by:

- DOD – Cyber Workforce Framework (DCWF)
- **European Commission** - The Cyber Resilience Act
- **CISA** - rolled out its initial, three-year comprehensive Strategic Plan of Action
- **EOP** - Chris DeRusha, Fed CISO, implemented a plan to enhance the security of the software supply chain to deliver a secure Government experience
- **NSA** – Cyber Collaboration Center providing free cybersecurity services to the DIB focused on small to medium-sized DOD contractors

The DoD Cyber Workforce Framework (DCWF)

The DCWF leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCT&CS). It has a hierarchical structure with seven broad categories, 33 specialty areas, and 54 work roles.

15

February 15, 2023

CISA Three-Year Strategic Plan of Action

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) rolled out its initial comprehensive plan of action to focus on and guide the agency's efforts over the next three years. **The Strategic Plan** communicates the agency's mission and vision promotes the unity of effort across the agency and partners, and defines success for CISA as an agency. It also describes the stakeholder, policy, and operational context 'in which we must perform and presents the strategic changes CISA will make to better execute our vital mission over the next three years.'

The [CISA 2023-2025 Strategic Plan](#) represents a forward-leaning, unified approach to achieving the agency's vision of ensuring secure and resilient critical infrastructure for the American people.

EOP - Chris DeRusha, Fed CISO, plan to enhance the security of the software supply chain

“The Biden-Harris Administration is committed to delivering a Government that works for all Americans – and technology powers our ability to do so. In order for Federal agencies to provide critical services, information, and products to the American people, they need access to secure and reliable software that manages everything from tax returns to veterans’ health records. That’s why the Office of Management and Budget is issuing guidance to ensure Federal agencies utilize software that has been built following common cybersecurity practices.’

NSA – Cyber Collaboration Center providing free cybersecurity services to the DIB

With the strong support of the DoD, CIO, NSA now offers free cybersecurity services to the DIB, including; shared threat intelligence, Protective Domain Name System, and vulnerability scanning services. They are also going to be piloting a series of new services over the next couple of years to see what works in terms of government-provided cybersecurity for the DIB, particularly trying to help those small-medium businesses that may not be able to afford world-class cybersecurity services on their own. Any organization that holds a DoD contract and related controlled information is eligible. All of the major primes are somewhat aware of these services.

- *Kristina P. Walter Chief, DIB Defense Cybersecurity Collaboration Center, National Security Agency*

Office of The National Cyber Director (ONCD)

ONCD is working to ensure every American can share in the full benefits of our digital ecosystem, including the economic prosperity and democratic participation it enables, while aggressively addressing and mitigating the risks and threats at large in cyberspace. By cultivating unity of purpose and efforts across agencies and sectors, ONCD will contribute to the development and implementation of stronger national strategy, policy, and resilience for our digital ecosystem

19

Office of National Cyber Director Principal Outcomes

The ONCD will realize this vision and execute the Biden-Harris Administration's cyber agenda by seeking to achieve four principal outcomes:

- Ensuring federal coherence
- Improving public-private collaboration
- Aligning resources to aspirations
- Increasing present and future CYBER Resilience

Office of National Cyber Director Principal Outcomes

The ONCD has issued three principal reports:

- The National Cybersecurity Strategy
- The National Cybersecurity Strategy Implementation Plan
- The National Cybersecurity Workforce and Education Strategy

Office of National Cyber Director Principal Outcomes

In March 2023, the White House issued **the National Cybersecurity Strategy**, outlining how the administration will manage the nation's cybersecurity through five pillars. This strategy seeks to build and enhance collaboration around five pillars:

- (1) Defend Critical Infrastructure,
- (2) Disrupt and Dismantle Threat Actors,
- (3) Shape Market Forces to Drive Security and Resilience,
- (4) Invest in a Resilient Future, and
- (5) Forge International Partnerships to Pursue

Office of National Cyber Director Principal Outcomes

National Cybersecurity Strategy Implementation Plan

All Americans deserve the full benefits and potential of our digital future. The

Biden-Harris Administration's National Cybersecurity Strategy calls for two fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace:

Ensuring that the biggest, most capable and best-positioned entities — in the public and private sectors — assume a greater share of the burden for mitigating cyber risk

Increasing incentives to favor long-term investments into cybersecurity

Office of National Cyber Director Principal Outcomes

The White House issued the **National Cybersecurity Workforce and Education Strategy** on August 1.

Why it matters: we only have enough people to fill about 70% of the jobs that are available.

This is causing stress, not only in the hiring platform, but also at the workplace due to overwork for those who are in the industry. The report makes it clear that this is a national security, imperative, and an economic imperative. It is also a human security, imperative.

Cyber also offered a Career and the pathway into well-paying professional jobs

The Office of the National Cyber Director's workforce strategy is broken into three pillars, focused on digital literacy, cybersecurity education and workforce issues.

Key Cyber Areas Closest to My Heart

To focus on our CYBER industry as a nation, we must:

- Inspire greater participation in our industry
- Provide a more even playing field so more minorities and women have a better chance to join our burgeoning industry
- We must make CYBER EDUCATION more accessible at every age from Grade 5 on up
- Explain our industry better

"LET US THEREFORE BRACE OURSELVES
TO OUR DUTIES AND BEGIN IN EARNEST
TO WORK TOGETHER & BUILD CYBER
FIRST AND LAST IN ALL THAT WE DO- AND
IF THE FREE PEOPLE OF THE USA AND
THE WORLD KEEP²⁶ A PEACE FOR A
THOUSAND YEARS, PEOPLE WILL SAY,
"THIS WAS THEIR FINEST HOUR."

Special Thanks & Recognition to Chris Inglis



“Time and tide wait for no
one.”

– Scottish Proverb

28

Thank you for joining us.