

CYBERSECURITY LESSONS FROM THE PANDEMIC

CSC White Paper #1



UNITED STATES OF AMERICA
CYBERSPACE
SOLARIUM
COMMISSION

CO-CHAIRMEN

Senator Angus King (I-Maine)

Representative Mike Gallagher (R-Wisconsin)

MAY 2020

SUMMARY/OVERVIEW

CSC WHITE PAPER #1 CYBERSECURITY LESSONS FROM THE PANDEMIC

KEN ZALEVSKY

CHIEF EXECUTIVE OFFICER

VIGILANT OPS, INC.



ABOUT VIGILANT OPS, INC.

- Vigilant Ops is a medtech company specializing in medical device security and the developer of the InSight Platform
- The InSight Platform is used by Medical Device Manufacturers to automatically generate, maintain and share Software Bill of Materials (SBOM)
- The InSight Platform is used by Healthcare Delivery Organizations to consume SBOMs and monitor deployed device vulnerabilities

CYBERSPACE SOLARIUM COMMISSION FINAL REPORT – MARCH 2020



- 2019 National Defense Authorization Act chartered CSC in 2019
- US President and Congress tasked CSC with two questions
 - What strategic approach will defend the United States against cyberattacks of significant consequence?
 - What policies and legislation are required to implement that strategy?
- Published Final Report on March 11, 2020 – 80+ recommendations
- 2021 Fiscal Year Legislative Proposals on July 14, 2020 – 54 legislative proposals
- ***“The status quo in cyberspace is unacceptable.”***
- ***“Adversaries are increasing their cyber capabilities while US vulnerabilities continue to grow.”***
- ***“If the US government cannot find a way to seamlessly collaborate with the private sector to build a resilient cyber ecosystem, the nation will never be secure.”***

PURPOSE OF THE WHITEPAPER

- Present cybersecurity challenges created by the pandemic
- Catalog lessons from the pandemic that can be applied to cybersecurity
- Provide new recommendations based on this insight
- Present revisions/updates to original recommendations from Final Report based on pandemic lessons



The background is a dark blue gradient. In the four corners, there are white, stylized circuit board traces. These traces consist of straight lines that turn at right angles, ending in small white circles, resembling electronic components or nodes on a network.

CYBERSECURITY CHALLENGES DURING A PANDEMIC

DIGITIZATION OF CRITICAL SERVICES

- **Summary** – social distancing has forced businesses online and government sustenance programs have revealed their infrastructural weakness, relying on antiquated software and systems
- **CSC Final Report - Recommendation 4.5.1 – Uptake of cloud services**
 - Incentivize the uptake of secure cloud services for small and medium-sized businesses and state, local, tribal and territorial governments
 - Grants to state governments for moving to cloud infrastructure
 - Second round of grants based on a competitive application system



WORK-FROM-HOME ECONOMY

- **Summary** – the massive shift to remote work has forced reliance on vulnerable home networks and personal devices as part of core business infrastructure
- **NEW Recommendation - pass an IOT security law**
 - Law should focus on known security challenges
 - Mandate reasonable security measures
 - NIST – “Recommendations for IoT Manufacturers” (references **SBOM** to communicate device components with customers)



WORK-FROM-HOME ECONOMY

- **Summary** – the massive shift to remote work has forced reliance on vulnerable home networks and personal devices as part of core business infrastructure
- **CSC Final Report Recommendation 4.1- establish labeling authority**
 - Expedited creation of National Cybersecurity Certification and Labeling Authority (references **SBOM** as a communication tool)
 - Expand scope of certification and labeling activities
 - Include consumer and personal electronics



WORK-FROM-HOME ECONOMY

- **Summary** – the massive shift to remote work has forced reliance on vulnerable home networks and personal devices as part of core business infrastructure
- **CSC Final Report Recommendation 4.2- establish liability for final goods assemblers**
 - Technology equipment manufacturers held liable for known vulnerabilities
 - Liability incentivizes adoption of better monitoring and patching practices



WORK-FROM-HOME ECONOMY

- **Summary** – the massive shift to remote work has forced reliance on vulnerable home networks and personal devices as part of core business infrastructure
- **CSC Final Report Recommendation 4.5.2 – develop a strategy to secure foundational internet protocols and email**
 - Security of the internet is imperative, particularly during crisis



COMBAT OPPORTUNISTIC CYBERCRIME

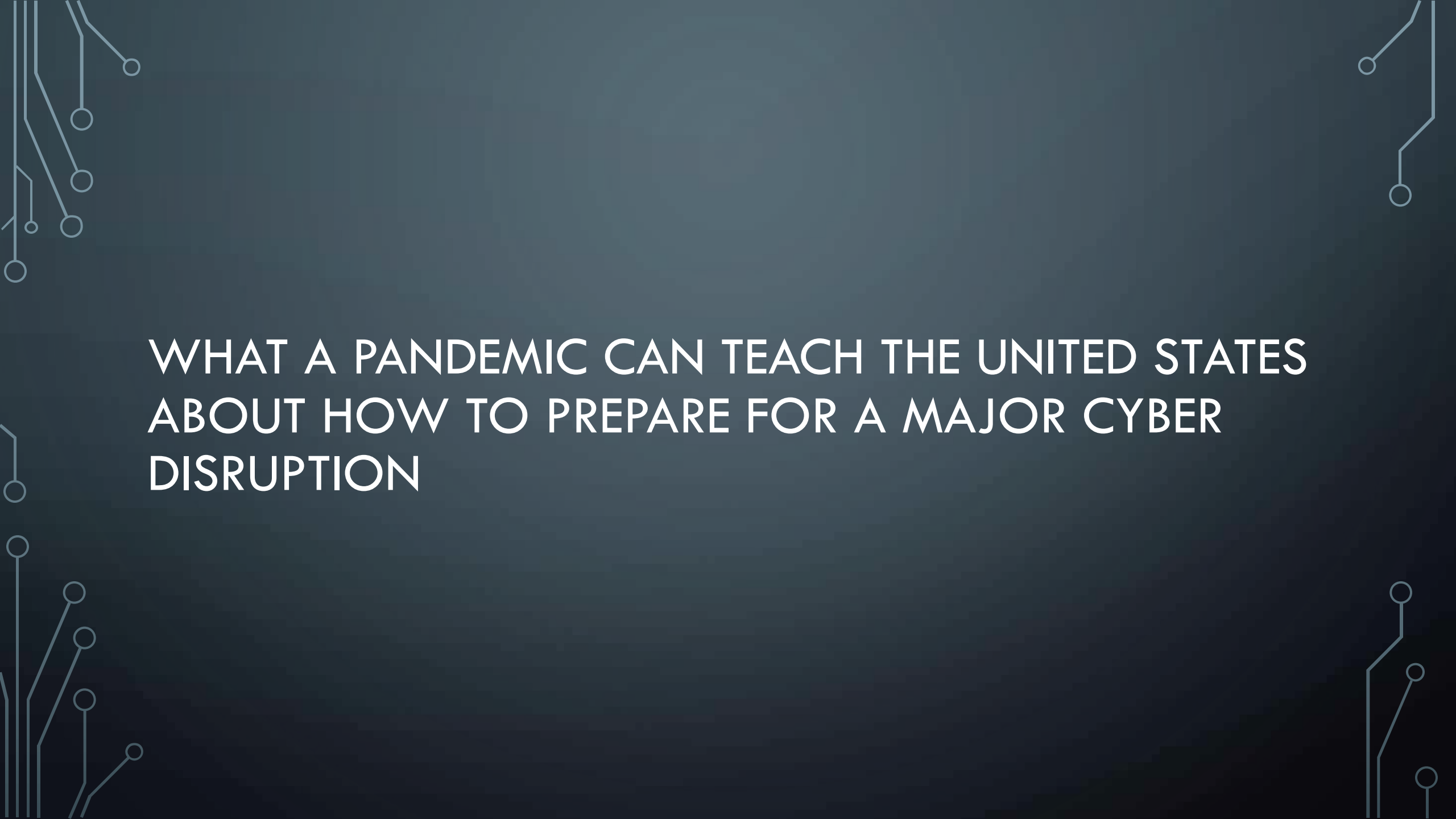
- **Summary** – during times of crisis, bad actors are emboldened to exploit susceptible victims and security vulnerabilities.
- **CSC Final Report Recommendation 1.4.2- strengthen the FBI's cyber mission and the National Cyber Investigative Joint Task Force**
 - Support a robust law enforcement and domestic intelligence response
 - Enhance long-term investigative capabilities



COMBAT OPPORTUNISTIC CYBERCRIME

- **Summary** – during times of crisis, bad actors are emboldened to exploit susceptible victims and security vulnerabilities.
- **NEW Recommendation** – support non-profits that assist law enforcement's cybercrime and victim support efforts
 - Cyber-specific non-profits have expertise to help in a crisis
 - Provide grants to enable financial stability and long-term viability



The background is a dark blue gradient. In the four corners, there are decorative white line-art elements resembling circuit traces or network connections, with small circles at the end of the lines.

WHAT A PANDEMIC CAN TEACH THE UNITED STATES ABOUT HOW TO PREPARE FOR A MAJOR CYBER DISRUPTION

EXECUTIVE BRANCH LEADERSHIP AND COORDINATION

- **Summary** – a national response to a significant cyberattack relies on a capable, experienced government management team with established relationships in the private sector and in state and local governments, as well as on having effective, tested programs, plans, and procedures in place.
- **CSC Final Report - Recommendation 1.3 – establish a national cyber director**
 - Act as the President’s principal advisor for cybersecurity
 - Head development of the national cybersecurity strategy
 - Coordinate incident response activities



EXECUTIVE BRANCH LEADERSHIP AND COORDINATION

- **Summary** – a national response to a significant cyberattack relies on a capable, experienced government management team with established relationships in the private sector and in state and local governments, as well as on having effective, tested programs, plans, and procedures in place.
- **CSC Final Report - Recommendation 1.4 – strengthen the Cybersecurity and Infrastructure Security Agency (CISA)**
 - Federal agencies must be sufficiently resourced and prepared to respond and lead during times of crisis



PLANNING FOR CONTINUITY OF THE ECONOMY

- **Summary** – the US has robust plans in place for continuity of operations and government, but not for the economy. Disruptions to the US economy has national and global impact
- **CSC Final Report - Recommendation 3.2 – develop and maintain continuity of the economy planning**
 - Initiate continuity planning with companies that produce and distribute critical goods and services
 - Ensure the continuous flow of goods and services



QUICK, EFFECTIVE, AND COORDINATED GOVERNMENT RESPONSE

- **Summary** – the US government must bolster its planning and coordination mechanisms to ensure a quick and effective response
- **CSC Final Report - Recommendation 5.4 – establish a Joint Cyber Planning Cell under Cybersecurity and Infrastructure Security Agency**
 - Plans for coordinated action between government and private sector
 - Develop comprehensive policies supporting an effective response



QUICK, EFFECTIVE, AND COORDINATED GOVERNMENT RESPONSE

- **Summary** – the US government must bolster its planning and coordination mechanisms to ensure a quick and effective response
- **CSC Final Report - Recommendation 3.33 – improve and expand planning capacity and readiness for cyber incident response and recovery efforts**
 - Clarify roles and responsibilities
 - Conduct cyber exercises (recommendations 3.3.4 and 3.35)



INTERNATIONAL COORDINATION

- **Summary** – cyber crises are inherently cross-border problems and require international cooperation and action
- **CSC Final Report - Recommendation 2.1** – create a **Cyber Bureau and Assistant Secretary at the US Dept of State**
 - Strong State Department leadership is critical
 - Coordinate an international response



INTERNATIONAL COORDINATION

- **Summary** – cyber crises are inherently cross-border problems and require international cooperation and action
- **CSC Final Report - Recommendation 2.1.1** – strengthen norms of responsible state behavior in cyberspace
 - Strong norms are critical for shaping behavior, preventing further harm, and stabilizing the environment during a crisis



INTERNATIONAL COORDINATION

- **Summary** – cyber crises are inherently cross-border problems and require international cooperation and action
- **CSC Final Report - Recommendation 2.1.3** – improve cyber capacity building and consolidate the funding of cyber foreign assistance
 - State Department building of capacity in partner nations to address state-sponsored hacking operations



AVAILABILITY AND SECURITY OF CRITICAL RESOURCES

- **Summary** – understanding and mitigating supply chain dependencies to prevent shortfalls in production capacity of goods and services
- **CSC Final Report - Recommendation 4.6 – develop and implement an Information and Communications Technology Industrial Base Strategy**
 - Prevent shortages of critical resources by identifying critical dependencies and ensuring adequate investment



AVAILABILITY AND SECURITY OF CRITICAL RESOURCES

- **Summary** – understanding and mitigating supply chain dependencies to prevent shortfalls in production capacity of goods and services
- **CSC Final Report - Recommendation 3.3.1 – design responsibilities for cybersecurity services under the Defense Production Act**
 - Enable the federal government to allocate critical cyber incident response services



A ROBUST FEDERAL CYBERSECURITY WORKFORCE

- **Summary** – following a significant cyberattack, the US will need to rely on a skilled cybersecurity workforce
- **CSC Final Report - Recommendation 1.5 – diversify and strengthen to Federal cybersecurity workforce**
 - Congress should immediately authorize additional flexibility to use direct hire authorities
 - Federal agencies should rapidly deploy apprenticeship programs for cyber roles



VOTER SAFETY AND SECURE, CREDIBLE VOTING

- **Summary** – American democracy depends on elections occurring on a fixed schedule
- **CSC Final Report - Recommendation 3.4** – improve the structure and enhance funding of the Election Assistance Commission (EAC)
 - EAC has the necessary expertise to address election challenges
 - EAC must be strengthened and better resourced



SUSTAINED NATIONAL RISK ASSESSMENT AND MANAGEMENT

- **Summary** – the nation must invest in systems that better forecast, rank, and manage risk to enable decisions makers to prioritize resources and increase resilience
- **CSC Final Report - Recommendation 3.1 – codify sector-specific agencies into law as Sector Risk Management Agencies and strengthen their ability to manage critical infrastructure risk**
 - Establishing basic expectations and responsibilities will provide the foundation for greater resources, authority, and accountability



SUSTAINED NATIONAL RISK ASSESSMENT AND MANAGEMENT

- **Summary** – the nation must invest in systems that better forecast, rank, and manage risk to enable decision makers to prioritize resources and increase resilience
- **CSC Final Report - Recommendation 3.1.1** – establish a five-year national risk management cycle culminating in a critical infrastructure resilience strategy



SUSTAINED NATIONAL RISK ASSESSMENT AND MANAGEMENT

- **Summary** – the nation must invest in systems that better forecast, rank, and manage risk to enable decisions makers to prioritize resources and increase resilience
- **CSC Final Report - Recommendation 3.1.2** – establish a **National Cybersecurity Assistance Fund** to ensure **consistent and timely funding** for initiatives that **underpin national resilience**



THE CRITICAL NEED FOR DATA

- **Summary** – the US cannot meaningfully prevent, manage, or mitigate future significant cyberattacks if it lacks data, models and forecasts
- **CSC Final Report - Recommendation 2.1.6 – improve attribution analysis and the attribution-decision rubric**
 - Help determine responsible parties and formulate a comprehensive response



THE CRITICAL NEED FOR DATA

- **Summary** – the US cannot meaningfully prevent, manage, or mitigate future significant cyberattacks if it lacks data, models and forecasts
- **CSC Final Report - Recommendation 4.3 – establish a Bureau of Cyber Statistics**
 - Create a central capacity empowered to collect and provide statistical data to empower and inform policymakers, the private sector, the general public, and the research community



THE CRITICAL NEED FOR DATA

- **Summary** – the US cannot meaningfully prevent, manage, or mitigate future significant cyberattacks if it lacks data, models and forecasts
- **CSC Final Report - Recommendation 4.4.1** – establish a public-private partnership on modeling risk



THE CRITICAL NEED FOR DATA

- **Summary** – the US cannot meaningfully prevent, manage, or mitigate future significant cyberattacks if it lacks data, models and forecasts
- **CSC Final Report - Recommendation 5.2 – establish and fund a joint collaborative environment for sharing and fusing threat information**
 - Ensure the continual collection and dissemination of relevant data and metrics to owners and operators of critical infrastructure
 - Collect data through a national cyber reporting law (Recommendation 5.2.2) and a national data breach notification law (Recommendation 4.7.1) as well as data collected via expanded and standardized voluntary threat detection programs (Recommendation 5.2.1)



GOVERNMENT CAPACITY TO RESPOND TO CRISES

- **Summary** – federal agencies are not sufficiently empowered to respond to a significant cyberattack
- **CSC Final Report - Recommendation 3.3 – codify a “Cyber State of Distress” tied to a “Cyber Response and Recovery Fund”**
 - The fund would allow for rapid mobilization and deployment of resources to assist governments and the private sector beyond what is available through conventional technical assistance and cyber response programs



GOVERNMENT CAPACITY TO RESPOND TO CRISES

- **Summary** – federal agencies are not sufficiently empowered to respond to a significant cyberattack
- **CSC Final Report - Recommendation 3.3.6** – clarify the cyber capabilities and strengthen the interoperability of the National Guard and assess the establishment of a military cyber reserve (Recommendation 6.1.7)



CREATING SOCIETAL RESILIENCE TO DISINFORMATION

- **Summary** – education helps to equip Americans to recognize disinformation operations, so they will be less susceptible to them
- **CSC Final Report - Recommendation 3.5 – build societal resilience to foreign malign cyber-enabled information operations**
 - Through literacy and modernized civic education, assist the average American to discern trustworthiness of online content



IDENTIFYING AND COUNTERING DISINFORMATION

- **Summary** – education helps to equip Americans to recognize disinformation operations, so they will be less susceptible to them
- **NEW Recommendation** – establish the **Social Media and Data Threat Analysis Center**
 - Independent, non-profit organization intended to encourage public-private cooperation to detect and counter foreign influence operations against the US



IDENTIFYING AND COUNTERING DISINFORMATION

- **Summary** – education helps to equip Americans to recognize disinformation operations, so they will be less susceptible to them
- **NEW Recommendation** – increase non-governmental capacity to identify and counter foreign disinformation and influence campaigns
 - Fund non-profit centers to identify, expose, and explain malign foreign influence campaigns to the American public



The image features a dark blue background with white, stylized circuit board traces in the corners. These traces consist of straight lines and small circles, resembling electronic components or data paths. The text is centered in a clean, white, sans-serif font.

WHILE COVID-19 IS THE ROOT CAUSE OF TODAY'S
CRISIS, A SIGNIFICANT CYBERATTACK COULD BE THE
CAUSE OF THE NEXT.

IF THAT PROVES TO BE THE CASE, HISTORY WILL SURELY
NOTE THAT THE TIME TO PREPARE WAS NOW.

TAKEAWAYS FOR MEDICAL DEVICE MANUFACTURERS

- CSC recommending fast-tracking critical security activities
 - Product labeling, which includes **Software Bill of Materials (SBOM)**
 - Reliance on standards, such as NISTIR 8259, which recommends **SBOM** as a communication tool
- Be ready to provide **SBOM** with products
 - Develop and implement SBOM processes
 - Generate and maintain SBOMs for each unique product version
 - Monitor SBOM component vulnerabilities
 - Share SBOMs with authorized end users

RESOURCES

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, FDA, October 2018 <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices>
- Postmarket Management of Cybersecurity in Medical Devices, FDA, December 2016 <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices>
- NTIA SBOM - <https://www.ntia.doc.gov/SoftwareTransparency>
- NEMA MDS² - <https://www.nema.org/Standards/view/Manufacturer-Disclosure-Statement-for-Medical-Device-Security>
- Cyberspace Solarium Commission - <https://www.solarium.gov>
- NISTIR 8259 Foundational Cybersecurity Activities for IOT Device Manufacturers - <https://csrc.nist.gov/publications/detail/nistir/8259/final>
- Vigilant Ops – www.vigilant-ops.com