NIAC The President's National Infrastructure Advisory Council

Actionable Cyber Intelligence: An Executive-Led Collaborative Model

DECEMBER 2020

Table of Contents

About the NIAC

The President's National Infrastructure Advisory Council (NIAC) is composed of senior executives from industry and state and local government who own and operate the critical infrastructure essential to modern life. The Council was established by executive order in October 2001 to advise the President on practical strategies for industry and government to reduce complex risks to the designated critical infrastructure sectors.

At the President's request, NIAC members conduct in-depth studies on physical and cyber risks to critical infrastructure and recommend solutions that reduce risks and improve security and resilience. Members draw upon their deep experience, engage national experts, and conduct extensive research to discern the key insights that lead to practical federal solutions to complex problems.

For more information on the NIAC and its work, please visit: cisa.gov/niac

National Security Council Tasking and Working Group Approach

In its December 2019 study, *Transforming the U.S. Cyber Threat Partnership*, the NIAC recommended that the President establish a **Critical Infrastructure Command Center (CICC) to improve real-time sharing and processing of private and public risk data—including classified information—between co-located government intelligence analysts and cleared cyber experts from companies whose functions are integral to U.S. national security**. The situation is dire and existing information sharing and partnership structures are neither agile enough nor tactical enough to respond to a cyber attack with the necessary speed.

Following the study's release, the CICC concept received considerable interest and support. The Cyberspace Solarium Commission referenced the NIAC's 2019 study in its March 2020 report, specifically citing the "need to partner with the owners and operators of the most critical infrastructure and improve intelligence sharing between government and industry."[1]

In February 2020, the National Security Council (NSC) determined that additional detail was needed. It instructed the NIAC to conduct a follow-on analysis to: 1) demonstrate the value that the CICC could provide, 2) identify CICC-related challenges that must be addressed, and 3) recommend an approach to achieve CICC operational functionality.

Working Group Approach

The NIAC's 2019 study recommended a series of actions **focused on the most at-risk entities and functions within the energy, financial services, and communications sectors**—those entities where a successful cyber attack could threaten public health and safety, national or regional economic stability, and the security of the nation. The central premise of the 2019 study and this subsequent effort is **that government and industry must work together in a new and different way**.

A Working Group of six NIAC members, including four members from the previous study, built on the *Transforming the U.S. Cyber Threat Partnership* report, previous NIAC studies, and the work of other relevant organizations to examine how to best operationalize the CICC concept. The Working Group interviewed 14 organizations to gather information on current efforts and better articulate the distinct value the CICC could add (see Appendix B for the list of contributors).

Given the NSC's guidance, the Working Group decided to develop a concept of operations that the White House could use to inform a phased implementation of the CICC. The Working Group details how the CICC will establish and operate, recognizing that, in practice, it is more important for the CICC to achieve the intended outcome than the specific names and mechanics presented here.

Within this study, references to the "private sector" or "companies" encompass any infrastructure that is not federally owned and/or operated, including state or municipal entities, and organizations of all sizes.

[1] Cyberspace Solarium Commission, *Final Report* (2020), pg. 144, https://www.solarium.gov/.

Concept of Operations

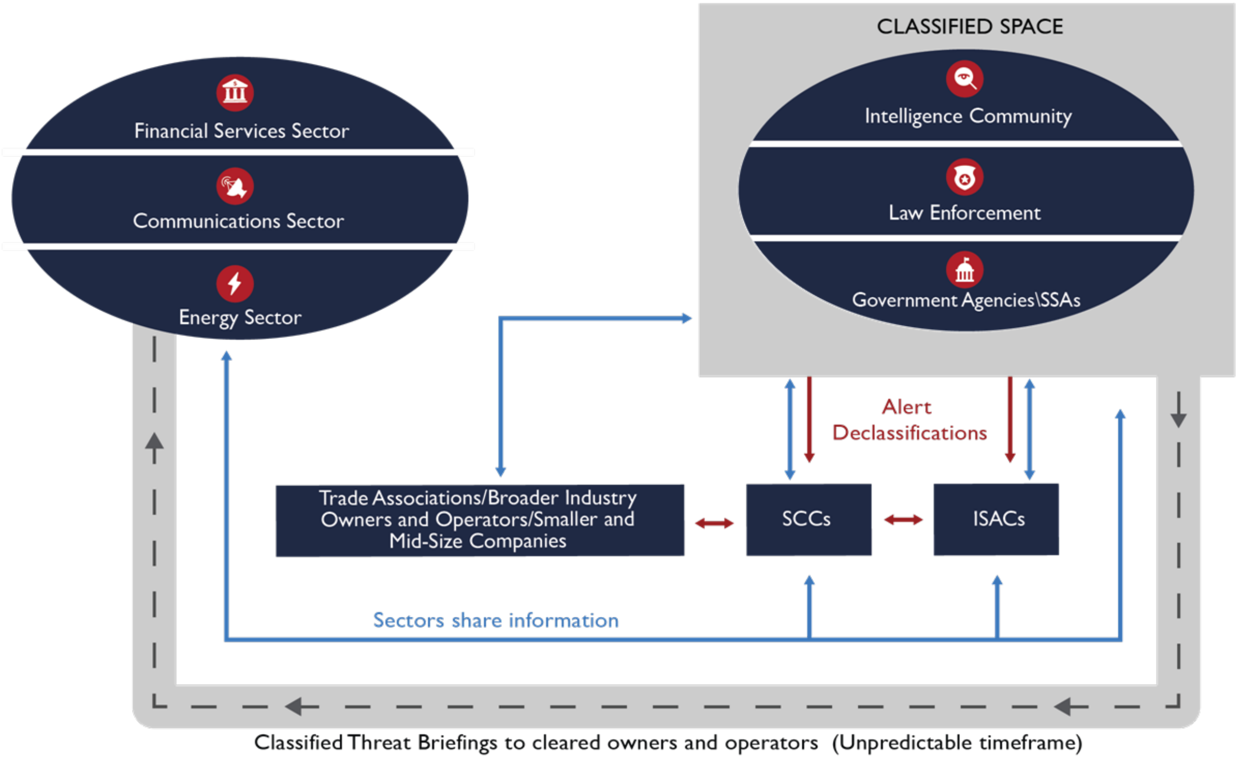
This concept of operations outlines an approach for implementing the CICC concept—including how the CICC would leverage and improve upon existing information and intelligence sharing, the additional value it would provide, and the challenges it will need to overcome to be successful.

Justification for Collaborative Change

The *2019 Worldwide Threat Assessment* reported that China and Russia now have the ability to execute cyber attacks that could disrupt U.S. critical infrastructure systems, and Iran has been preparing for cyber attacks against the United States and our allies.[2] Recent high-profile attacks—WannaCry, NotPetya, Industroyer, CrashOverride, Triton/Trisis—demonstrate the growing ability of our adversaries to disrupt, deny, and destroy critical infrastructure from thousands of miles away. An attack that successfully disrupts critical sectors could jeopardize lives, our economy, and U.S. national security.

Existing intelligence sharing between government and industry does not move at the speed required to prevent, mitigate, or respond to the most serious cyber threats to the most critical infrastructure systems.

Figure 1. Existing Public-Private Intelligence Sharing


CLASSIFIED SPACE
Intelligence Community
Law Enforcement
Government Agencies\SSAs
Financial Services Sector
Communications Sector
Energy Sector
Alert
Declassifications
Trade Associations/Broader Industry Owners and Operators/Smaller and Mid-Size Companies
SCCs
ISACs
Sectors share information
Classified Threat Briefings to cleared owners and operators (Unpredictable timeframe)

The absence of direct collaboration and innovation with the private sector creates intelligence gaps: government cyber threat data often lacks the context and transparency to determine how an attack could

[2] Daniel R. Coats, "Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community," Before the Senate Select Committee on Intelligence, January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

manifest in infrastructure systems or the potential magnitude of damage or disruption. This delays the federal government's ability to translate aggressive cyber threats into actionable mitigation measures and distinguish those threats that pose the greatest risks to national security. This gap creates the potential to over- or under-estimate a cyber threat and hinders appropriate federal and industry response.

CICC Mission and Operations

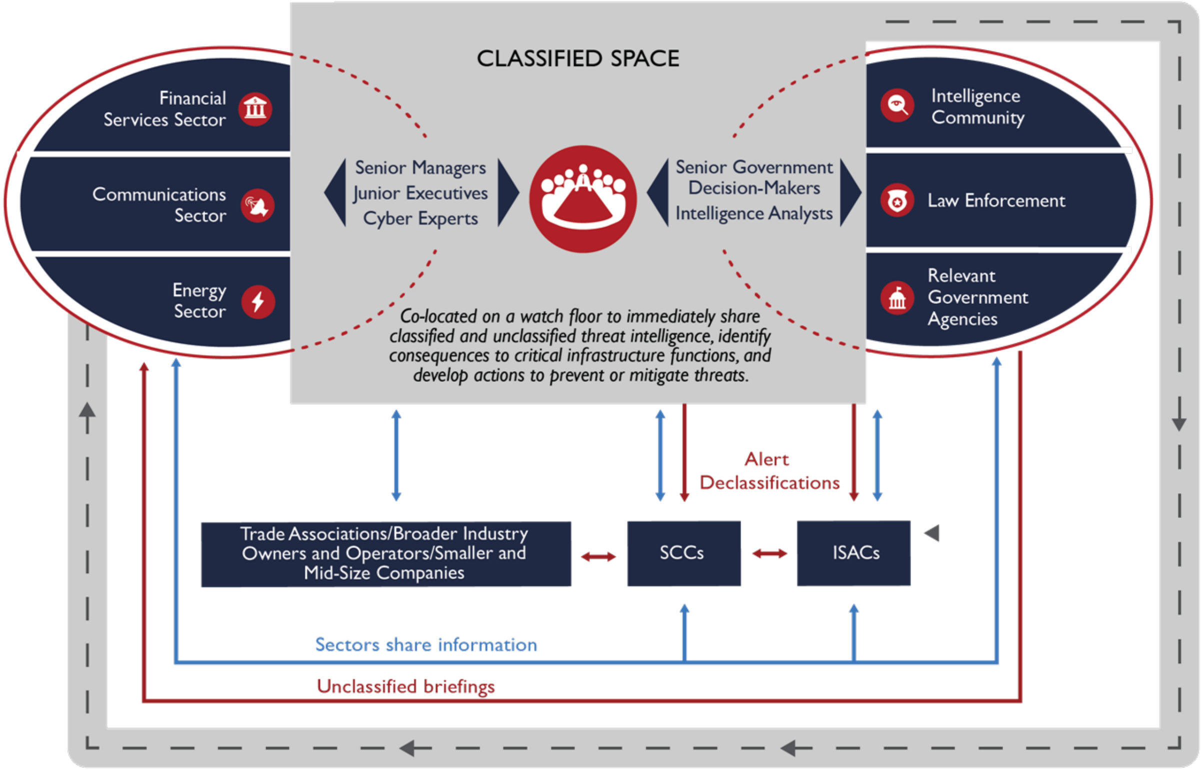
The CICC is not simply another cyber intelligence or information sharing mechanism; rather, it is an operations center intended to drive innovative, tactical, and rapid solutions to cyber threats affecting the infrastructure most critical to U.S. national security and the U.S. economy.

Moreover, the CICC should be founded by private sector executives, who task senior managers with relevant experience to participate in a 24/7 watch floor with their public sector colleagues. Working side-by-side in a classified environment, government and industry experts can rapidly assess intelligence in real-time and then develop and communicate tactical measures to protect critical infrastructure systems. By focusing first on a subset of the most critical companies in three highly targeted sectors, the CICC has the distinct agility, authority, and expertise to mitigate imminent threats to national security.

CICC MISSION

Establish a public-private collaborative space in which government and private sector experts work in concert to collect, process, and analyze cyber threat information; assess risks to critical sector operations; and rapidly disseminate pertinent tactical information or intelligence to effectively apply prevention or mitigation measures in the most highly critical infrastructure in the private sector.

Figure 2. CICC Concept Role in Relation to Existing Entities


CLASSIFIED SPACE
Financial Services Sector
Communications Sector
Energy Sector
Senior Managers
Junior Executives
Cyber Experts
Senior Government Decision-Makers
Intelligence Analysts
Intelligence Community
Law Enforcement
Relevant Government Agencies
Co-located on a watch floor to immediately share classified and unclassified threat intelligence, identify consequences to critical infrastructure functions, and develop actions to prevent or mitigate threats.
Alert
Declassifications
Trade Associations/Broader Industry Owners and Operators/Smaller and Mid-Size Companies
SCCs
ISACs
Sectors share information
Unclassified briefings

Distinct Capabilities and Requirements

The Working Group identified five initial distinct CICC capabilities. Associated requirements and operational characteristics are noted for each.

1. **Provide real-time, direct collaboration between government intelligence analysts and experts from the private sector** to efficiently identify, analyze, and mitigate national security level threats to highly critical sectors, with oversight and engagement of senior managers from private sector and government.

Requirements

- Co-locate senior private sector managers, company cyber experts, government managers, and government intelligence analysts working side-by-side at a 24/7 watch floor.
    - Private sector analysts with clearances sit on the watch floor and have access to company systems (e.g., through virtual private networks, cloud, and remote desktop).
    - Government managers and cyber analysts with clearances sit on the watch floor with access to Intelligence Community (IC) systems.
    - Weekly secure conference call to include extended partners who may not have a physical presence in the CICC.

Operational Characteristics

- Initial membership includes companies from the energy, financial services, and communications sectors. Other sectors can be added as the concept matures and grows.

2. **Develop innovative mitigation measures** by using the collective expertise of private sector CICC staff, government managers, and national experts to directly share with the broader critical infrastructure community (including ISACs and small and medium sized entities).

Requirements

- Ability to engage internal CICC staff and external expertise from National Labs, academia, vendors/service providers, etc. to rapidly develop, test, and disseminate mitigations and response actions, based on the severity of the threat.
    - Code, patches, tools, or other mitigation measures can be tested and validated within the CICC companies.
    - Mitigation measures can be shared and disseminated to the broader infrastructure community using industry partnerships like Information Sharing and Analysis Centers (ISACs) and Sector Coordinating Councils (SCCs).
- Perform effectiveness testing to meet leading industry practices and standards.
- Integrate threat modeling based on intelligence to identify systemic infrastructure risk and introduce new mitigation controls.

Operational Characteristics

- Analyze threat intelligence to prioritize risk, understand impact, and release code or various tools to help entities (including small- and medium-sized entities) make informed decisions to manage risk.

- Allow the private sector to better prioritize risk mitigation strategies given the limited private sector resources.

3. **Assess a threat or vulnerability's consequences to broader critical infrastructure sectors**, assist in issuing alerts that can be shared broadly, and share tools to help determine if the identified vulnerability is on a company's system.

Requirements

- Provide insight into the consequences of potential threats on company operations and broader implications across sectors.
- Identify the level of severity and inform government collection and response actions.
- Share threat indicators with other company analysts on the floor to identify prevalence of a threat indicator and/or to notify partners to be on alert.

Operational Characteristics

- Support rapid declassification of threat information and mitigations by identifying the minimal parts of intelligence needed for companies to act and share with sector partners and smaller entities (e.g., through ISACs and other mechanisms).
- Establish a responsible disclosure program for centralized critical infrastructure to share threats and indicators of compromise (IOCs).

4. **Monitor threat activity on infrastructure systems that could indicate targeting of a particular sector or device/system**, provide sector-specific insight to assess impacts to operations and supply chain, and inform appropriate government or company response.

Requirements

- Flag unusual activity or threat indicators in company systems and share them directly with government analysts without risks associated with data leaving company systems.
- Enrich intelligence collection and products with insight from private sector analysts.
- Evaluate threat data with continuous real-time monitoring to alert critical suppliers of CICC members.
- Provide a platform that enables the private and public sector to perform confidential cyber correlation searches.

Operational Characteristics

- Provide input to identified government entities to help determine appropriate government response, including potential legal or policy actions, depending on type of threat and actor involved (e.g., nation state vs. cyber criminals).

5. **Allow the Intelligence Community (IC) to quickly share threats and intelligence with private companies** and enable the private sector to add valuable context to support improved intelligence collection.

Requirements

- Government analysts have the mission and authority to collect intelligence on threats to privately owned critical infrastructure systems and make the private sector an explicit IC customer.

Operational Characteristics

- Utilize and enhance existing intelligence distribution methods to ensure rapid, concise, actionable intelligence.

Staffing Selection, Roles, and Responsibilities

The CICC is not intended to replace existing intelligence and information sharing mechanisms between government and industry. As illustrated in Figure 2, the CICC concept fills the gap in existing intelligence sharing where more direct coordination and collaboration is needed between government and industry.

CICC operations need experienced company and government managers and analysts who can quickly provide context to government intelligence and develop the necessary tools and mitigations. CICC staff will communicate recommendations (i.e., code, technology configurations, new controls) for immediate action to prevent or mitigate serious cyber threats. The CICC staff will be able to communicate these actions, with credibility, to the leaders of their respective companies.

The roles and responsibilities for each of the key players is outlined below, recognizing that additional detail will be needed for implementation.

CICC Member Companies

- Initial CICC Membership should include the companies with the most critical functions from the energy, financial services, and communications sectors.
- Member companies will provide employees and resources to establish and operate the CICC, including senior managers, junior executives, and cyber analysts to staff the 24/7 watch station.

CICC Staff

- Dedicated company and government senior leaders (C-suite level) should conduct a virtual weekly meeting to lead, manage, and direct the effective staffing and functioning of the CICC.
- Junior executives from initial CICC member companies and intelligence analysts and representatives from relevant agencies will provide guidance.
- CICC member companies will provide junior executives with the right capabilities and experience with company systems to understand the information/intelligence and its impact. In this role, they will help quickly provide insights to determine the necessary mitigation actions.
- CICC member companies will also provide cyber analysts to monitor their company networks and access a voluntary CICC data lake (in which member companies would share information, such as netflow or operational technology network data) to compare threat indicators.
- Intelligence analysts and engineers from multiple agencies in the IC would be engaged and representatives from the relevant federal agencies (e.g., SSAs) should be on the watch floor.

Stakeholders and Outside Experts

- Existing information sharing mechanisms will provide valuable input.
- National Labs, academia, vendors/service providers, and other experts will be engaged as needed to help develop innovative mitigations.
- Critical infrastructure owners and operators who are not CICC members and are not located physically onsite will participate in regular calls and briefings as appropriate.

Use Cases and Operational Scenarios

The Working Group explored three scenarios to illustrate how the CICC will operate in practice and the value it will provide. The scenarios include vulnerability identification and prioritization, a ransomware attack, and a successful cyber attack that results in a disruption to critical functions.

Scenario 1: Vulnerability Identification and Prioritization

PROBLEM

The National Institute of Standards and Technology (NIST) has documented more than 16,000 vulnerabilities each of the last two years, and the National Vulnerability Database is on pace to exceed 18,000 in 2020.[3] This equates to nearly 50 vulnerabilities every day that private sector analysts must review, assess for relevance and impact to company systems, and ultimately mitigate if necessary. Companies struggle to quickly identify which vulnerabilities affect their specific equipment and elevate those that pose the most significant risk to their critical systems. An effort to patch one vulnerability may take a team of analysts months to plan and execute, making it imperative to prioritize the highest risks.

CICC'S APPROACH

- Identify malicious behavior patterns that could indicate vulnerability targeting.
- Collaboratively prioritize vulnerabilities that affect critical sector systems and use private sector expertise to identify how those vulnerabilities could manifest to disrupt sector operations and achieve a national impact.
- Focus industry and government expertise and resources on developing code/tools that would help the private sector find and patch high-impact vulnerabilities. While CICC activities will never replace a robust vulnerability patching program, CICC actions can help alert companies to a more serious vulnerability and provide novel tools to quickly find it within their systems.

[3] "2019 in Review," National Vulnerability Database, News, accessed November 23, 2020. https://nvd.nist.gov/General/News/2019-in-Review

CICC VALUE

- **Better identify malicious behavior patterns across sectors** to elevate alerting and coordinate public-private response actions.
- **Improve application of the Common Vulnerability Scoring System** to accelerate sector-wide patching and mitigation of high-impact vulnerabilities.
  - The System includes 22 variables, and government analysts must make several assumptions to arrive at a score. Private sector analysts understand real-world asset inventories and operating environments, and can offer expertise to increase the specificity and value of the score. There may even be an opportunity to develop severity scores by sector, helping small or mid-sized companies better prioritize action.

Scenario 2: Ransomware or Zero-Day Malware

PROBLEM

Malware can give attackers unauthorized access and control in critical networks to cause disruption or damage. Malicious actors use ransomware—a form of malware—to encrypt and prevent access to a company's data or networks until a ransom is paid. According to the Federal Bureau of Investigation's Internet Crime Report, 2,047 reported ransomware attacks on U.S. organizations in 2019 resulted in "adjusted losses of over $8.9 million."[4]

Zero-day malware is a previously unknown software attack that security tools cannot yet detect; even for known threats, security software may not detect a ransomware payload, especially in the case of encrypted payloads. If an attack is suspected or detected in its early stages, immediate removal or isolation of the malware would likely stop encryption or reduce further data damage.

While these attacks can be costly or debilitating to an individual organization, the CICC cannot focus on mitigating all malware or ransomware threats. However, it can focus on identifying malicious behavior targeting critical sectors and malware vulnerabilities that could impact national security functions—while sharing indicators and mitigations that improve security sector-wide. Using software or other security policies to block known payloads from launching will help prevent malware. Software patches from vendors often mitigate ransomware vulnerabilities, so regular patching is also a key part of a mitigation strategy. Other mitigation measures include cyber hygiene and network segmentation. Still, there is no guaranteed prevention solution so having local and offline backups are a critical component to defending against ransomware.

CICC'S APPROACH

- Provide enriched intelligence in a classified environment that enables companies to proactively monitor critical networks, identify indicators to better detect malware, and identify targeting behavior that could warn of new malware exploits.
- Provide strategic analysis for ransomware/malware attacks on private sector critical networks and improve the ability of government to make threat actor attributions.

[4] Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report* (2020), https://pdf.ic3.gov/2019_IC3Report.pdf; Jeff Stone, "Ransomware to blame for nearly half the cyber-insurance claims filed in early 2020," *CyberScoop*, September 11, 2020, https://www.cyberscoop.cm/ransomware-cyber-insurance-cost-beazley-coalition/.

- Create and provide access to a secure, voluntary data lake for CICC member company staff and government analysts to conduct their own analysis.
    - For example, a company analyst that identifies a suspicious IP address can use the power of the data lake to scan netflow from other sector companies and correlate information to discern a threat. The analyst can rapidly report suspected threats to CICC partners, who can work collaboratively to scan for similar activity and identify a potential widespread exploitation campaign.
- Develop code that can be disseminated through ISACs and other existing information sharing mechanisms to quickly update malware detection signatures or patch malware vulnerabilities. A similar model is used by the United Kingdom's National Cyber Security Centre.

CICC VALUE

- **Improve the speed of mitigations and related malware prevention** while collaborating with the Intelligence Community to disseminate classified intelligence through Federal Bureau of Investigation notification or declassifying and releasing information through ISACs.
- **Provide private sector context to intelligence** to better measure the potential severity of malware targets and prioritize high risk trends for collection.

Scenario 3: Successful Cyber Attack that Disrupts Critical Functions

PROBLEM

A cyber attack that successfully disrupts critical infrastructure functions—particularly those integral to national security—requires a rapidly coordinated federal and private sector response to limit damage, protect other critical targets, and speed recovery.

CICC'S APPROACH

- Facilitate direct and immediate collaboration between private sector and government managers and analysts to develop innovative mitigation measures that can be shared in the broader critical infrastructure community, including with ISACs and small and medium-sized entities.
- Develop code and patches that can be disseminated through ISACs and put directly into private sector cybersecurity systems, which removes bureaucracy inherent in federal cyber response through Presidential Policy Directive 41 and enables an immediate detection of further malicious activity.
- Assess the consequences to broader critical infrastructure sectors, develop mitigations, and help declassify only pertinent information needed for an alert.

CICC VALUE

- **Improve tactical collaboration** by providing a classified space where the impacted companies and sectors can rapidly respond with government partners to address the threat and limit the impact of an attack.

Analysis of Proposed Solution

The distinct value of CICC coordination is to rapidly identify and test innovative, actionable solutions, and then transmit them to the broader critical infrastructure community.

Existing Information Sharing Mechanisms and Value Added

The CICC concept complements existing information sharing mechanisms (as illustrated in Figure 2). The table below highlights the functions provided by existing mechanisms and how the CICC concept adds value to current efforts.[5]

Existing Mechanisms	Functions	Added CICC Value
Information Sharing and Analysis Centers (ISACs)	• Sector-specific ISACs are nonprofit, member driven organizations formed by critical infrastructure owners and operators to share all-hazards threat information between government and industry. • The communications, electricity, and financial sectors each have their own ISACs with a 24/7 watch floor to collect, analyze, and disseminate information on vulnerabilities and threats.	• Add context to classified threat information using private sector insights. • Quantify the risk a threat poses to individual sectors and critical infrastructure as a whole. • Identify cross-sector trends by combining inputs from ISACs with other information sources (classified and unclassified). • Assist in developing alerts and tools that can be shared back to the ISACs for broader distribution. • Assess a threat or vulnerability's consequences to broader critical infrastructure sectors, assist in developing an alert that can be shared broadly, and provide tools to help identify vulnerabilities in company systems.
Government-Run Watch Floors	• Sector-Specific Agencies (SSAs), law enforcement, and the intelligence community run watch floors to monitor threats and malicious cyber activity; share threat information with relevant stakeholders and partners, and in some instances develop tools or provide technical assistance. • Examples include: o Cybersecurity & Infrastructure Security Agency (CISA) Central (formerly the National Cybersecurity and Communications Integration Center) o U.S. Cyber Command o NSA's Cybersecurity Directorate	• Streamline coordination and provide operational tools across government and industry organizations, serving to connect the broader cyber landscape across industries and government intelligence. • Increase understanding of the sector through private sector insights into how cyber threats could potentially impact company systems and potentially supporting faster declassification and dissemination through existing mechanisms.

[5] Please see references in Appendix C.

Existing Mechanisms	Functions	Added CICC Value
	○ Federal Bureau of Investigation (FBI) National Cyber Investigative Joint Task Force (NCIJTF)	
Regional Intelligence Centers	• Regional Intelligence Centers facilitate daily intelligence sharing among public safety and service agencies at the federal, state, local and tribal levels, and with critical infrastructure and key private sector resources. • Private sector partners work in classified space with government analysts to assess risk using unclassified data from critical infrastructure. ○ Mechanisms allow for private sector partners to reach back to the center's analyst to continue the investigation. • Examples include: ○ Kansas Intelligence Fusion Center ○ Michigan Intelligence Operations Center	• Expand scope to national and/or sector-wide context to IOCs and threats. • Add key IC partners to analysis process and capability.
Analysis and Resilience Center (ARC)	• Launched in October 2020 by financial and energy sector leaders, the ARC focuses on identifying strategic risk and provides a risk register to facilitate comprehensive analysis and mitigation.	• Provide operational component and develop innovative mitigation measures that are applied directly and shared with the broader critical infrastructure community. • Drive collection requirements and help prioritize necessary actions.

Existing International Models

The Working Group reviewed existing successful international models where government and industry collaborate to identify and mitigate cyber threats. While there are different governance structures in place, these organizations illustrate how public-private collaboration can work.

- **The United Kingdom's National Cyber Security Centre (NCSC)** serves as the public face of the United Kingdom's cybersecurity initiatives and a single point of contact for companies, other government agencies, and the general public. The NCSC provides guidance, responds to cybersecurity incidents, enhances cybersecurity capabilities, and secures public and private sector networks.[6]
  - The NCSC works closely with private sector partners to facilitate information flow and better understand risks and consequences to industry. This helps the NCSC refine risk recommendations and tailor guidance to different industries (e.g., the Industry 100

[6] "About the NCSC," National Cyber Security Centre, accessed November 6, 2020, https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.

program where company-funded representatives come and work at the NCSC on a part-time basis).[7]

- **The Australian Cyber Security Centre (ACSC)** monitors cyber threats to Australia and shares advice and information about cyber safety with individuals, critical infrastructure operators, and companies of all sizes. The ACSC also responds to cybersecurity threats as the Australian computer emergency response team (CERT).[8]
    - Under the Joint Cyber Security Centre (JCSC) program, ACSC partners with business, government agencies, academia, security vendors, and consulting firms to provide services and support, including cyber threat intelligence and a platform for collaboration and sharing.[9]
    - The ACSC has dedicated space for multi-classification environments and local centers are instrumental in making connections across public and private sectors.
    - Collaboration with the private sector is generally at the unclassified level. ACSC shares classified intelligence with some key partners.

Action Plan

The Working Group recommends the following near-term actions to implement the CICC concept:

1. The President should direct the relevant federal agencies to support the private sector in rapidly standing up the CICC concept with the energy, financial services, and communications sectors:
    a. Within 90 days the private sector will identify the executives who will lead execution of the CICC concept and establish governing criteria (including membership, staffing and rotation, and other logistics).
    b. Within 120 days the CICC sector executives will identify and assign the necessary CICC staff from the private sector.
    c. Within 90 days an appropriate venue to house the operational component will be identified and the necessary agreements put in place.
2. The President should direct the Intelligence Community and other relevant government agencies to identify and co-locate the required government staff counterparts to enable the direct coordination required by the CICC. This staff should be pulled from the IC, SSAs, and law enforcement.
3. The President, working with Congress, should establish the appropriate authorities and mission for federal agencies to directly share intelligence with critical infrastructure companies, along with any other authorities required for the CICC concept to be fully successful (identified in Appendix A).
4. Once the CICC concept is fully operational (within 180 days), the responsible executives should deliver a report to the NSC and the NIAC demonstrating how the distinct capabilities of the CICC have been achieved and the impact of the capabilities to date. The report should identify remaining gaps in resources, direction, or authorities.

[7] "Industry 100," National Cyber Security Centre, accessed November 20, 2020, https://www.ncsc.gov.uk/information/industry-100.

[8] "About," Australian Cyber Security Centre, accessed March 19, 2020, https://cyberexchange.uk.net/about-us/.

[9] "Joint Cyber Security Centres," Australian Signals Directorate, accessed May 20, 2020, https://www.cyber.gov.au/programs/joint-cyber-security-centres.

The CICC concept may take several years to reach full maturity and should remain small and agile in its early stage; but the Working Group believes that the initial facility, staff, agreements, and operations can be rapidly stood up—at the direction of private sector and government executives.

Appendix A: Available Authorities and Authorities Needed to Succeed

The National Security Council (NSC) asked the NIAC to determine the legal agreements required to implement the CICC concept and identify any gaps that might exist in current authorities. This appendix summarizes the results of the Working Group's examination of the existing authorities and the gaps to address for the CICC to fully achieve the operational functionality intended. **Ultimately, private and government entities must establish trusted relationships for the real-time, two-way sharing of threat information to be effective**.

Some of the current gaps that should be addressed to ensure the success of the CICC include:

- Liability protection to encourage private sector entities to share information about a breach;
- Clear guidance to facilitate the rapid declassification of intelligence; and
- Explicit directives to allow the Intelligence Community and relevant federal agencies to participate.

CICC Capabilities, Application of Existing Authorities, and Potential Gaps

The table below maps the CICC's distinct capabilities with existing authorities that could be leveraged and any gaps or limitations that may prevent full realization of the capabilities. Please note references to non-federal governmental entities include private sector organizations or companies, municipally owned and operated entities, and organizations of all sizes. Any subsequent references to the private sector or companies are intended to capture this group.

CICC Capability
1. **Provide real-time, direct collaboration between government intelligence analysts and experts from the private sector** to efficiently identify, analyze, and mitigate national security level threats to highly critical sectors, with oversight and engagement of senior managers from private sector and government.

Existing Authorities	Potential Gaps in Authorities
• **Cybersecurity Information Sharing Act of 2015 (CISA)** – Allows information sharing between the U.S. government and technology and management companies. Authorizes companies to monitor and implement defensive measures on their own information systems to counter cyber threats. • **Cybersecurity State Coordinator Act (2020**) – Directs the Cybersecurity and Infrastructure Agency (CISA) to improve the capacity of state and local governments to protect against cybersecurity threats. Improves intelligence	• **The Cybersecurity Information Sharing Act of 2015 is limited to sharing information and not mitigation efforts** that can be applied to the broader critical infrastructure community; also does not satisfy all federal reporting requirements. Regulators such as the FTC and SEC have stated that they consider cooperation and voluntary reporting favorably when pursuing enforcement actions. • **Cybersecurity State Coordinator Act** does not permit the Intelligence Community to share information with the private sector; does not

Existing Authorities	Potential Gaps in Authorities
sharing between state and federal governments. • **State and Local Government Cybersecurity Act (2019)** – Encourages national cybersecurity watchdogs to share information regarding cybersecurity threats, vulnerabilities, and breaches. Helps bolster all levels of government defense from sophisticated cyberattacks. • **Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013)** – Increases the volume, timeliness, and quality of cyber threat information sharing. • **Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (2013)** – Directs the creation of a situational awareness capability to address physical and cyber aspects of how critical infrastructure is functioning, understand the consequences of attacks to critical infrastructure, and improve the relationship between private critical infrastructure companies and government regulators to improve cybersecurity efforts. • **National Security Presidential Directive (NSPD) 54, Cybersecurity Policy (2008)** – Defines the federal cybersecurity role in critical infrastructure domains, developing global supply chain risk management, and coordinating research and development efforts; contained broad mandates, directing the Secretary of Homeland Security to "conduct outreach to the private sector on cybersecurity threat and vulnerability information." • **Defense Industrial Base Cybersecurity Program, pursuant to 32 CFR Part 236 (2007)** – Voluntary program that allows the Department of Defense to share classified and unclassified cyber threat information with defense industrial base participants in near real-time. • **Homeland Security Act of 2002** – Established within the Department of Homeland Security a Directorate for Information Analysis and Infrastructure Protection, which mandated,	provide real-time, side-by-side coordination; and is limited to state and local governments. • **State and Local Government Cybersecurity Act** is limited to state and local governments and does not provide real-time, side-by-side coordination. • **Executive Order 13636** stops short of creating new federal requirements, resources, or authorities to support systemically important critical infrastructure or additional expectations on the private-sector entities that receive it. • **Presidential Policy Directive 21** remains focused on federal government-led efforts to engage with private sector. • **NSPD 54** established broad policy objectives that have lost momentum with changes in administration, although the directive has not been repealed. • **Defense Industrial Base Cybersecurity Program** is limited to defense contractors and may have limited voluntary participation. • **Homeland Security Act** provides the foundational document and authorities for coordination between government entities and critical infrastructure owners; however, implementation of those authorities since the Act's passage has demonstrated that certain programs are still not optimally promoting public-private coordination. • **The Patriot Act authorizes** the CFTF construct, but the effectiveness of this program has been hampered by lack of funding; the CFTF also relies on trust from industry participants to facilitate victim notification.

Existing Authorities	Potential Gaps in Authorities
inter alia, that the Directorate receive and analyze law enforcement and intelligence information from federal, state, and local agencies and the private sector; carry out comprehensive assessments of vulnerabilities of critical infrastructures; and integrate relevant information, analyses, and vulnerability assessments to identify protection priorities. • **Patriot Act (2001)** – Provides authority for the Secret Service-led Electronic Crimes Task Force, which recently merged with the Financial Crimes Task Force to become the Cyber Fraud Task Force (CFTF); the CFTFs partner with over 4,000 private sector entities, 2,500 international, federal, state, and law enforcement partners, and 350 academic partners to share information and analysis on cyber-crimes with financial economic impact.	

CICC Capability
2. **Develop innovative mitigation measures** by using the collective expertise of private sector CICC staff, government managers, and national experts to directly share with the broader critical infrastructure community (including ISACs and small and medium sized entities).

Existing Authorities	Potential Gaps in Authorities
• **Cybersecurity State Coordinator Act (2020)** – Directs the Cybersecurity and Infrastructure Agency (CISA) to improve the capacity of state and local governments to protect against cybersecurity threats. Improves intelligence sharing between state and federal governments. • **Executive Order 13920: Securing the Bulk Power System (2020)** – Requires the Department of Energy to establish criteria for pre-qualified bulk power system equipment and further directs the Department of Energy to identify existing bulk power system equipment that poses a risk to national security, developing recommendations to isolate or replace that equipment as appropriate.	• **Cybersecurity State Coordinator Act** is limited to state and local governments; does not provide mitigation measures; and is not specific to the broader critical infrastructure community. • **Executive Order 13920** is motivated by concern with Huawei and ZTE components in the bulk power system and focuses on remediating that immediate concern through identification of criteria rather than on promoting innovative technologies per se; does not address distribution system as outside of federal purview. • **State and Local Government Cybersecurity Act** is limited to state and local governments; and is limited to the collaboration and access to

Existing Authorities	Potential Gaps in Authorities
• **State and Local Government Cybersecurity Act (2019)** – Encourages national cybersecurity watchdogs to share information regarding cybersecurity threats, vulnerabilities, and breaches. Helps bolster all levels of government defense from sophisticated cyberattacks. • **Sarbanes-Oxley Act (SOX) of 2002 and SEC Statement and Guidance on Public company Cybersecurity Disclosures (2018)** – Section 404 of SOX requires public companies to report on the effectiveness of internal controls over financial reporting and an auditor's attestation as to the effectiveness of the internal control structure; such internal controls include IT controls. The SEC's recent Statement and Guidance on these disclosures assists public companies in preparing disclosures about cybersecurity risks and incidents. Advises companies to implement comprehensive policies and procedures to respond to cyber risks and incidents. • **Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017)** – Supports cybersecurity efforts of critical infrastructure entities. Classified report published pursuant to Executive Order 13800 indicates that DHS seeks to improve access to classified information for critical infrastructure owners and operators and improve incident communication and coordination. • **Presidential Policy Directive 41 (2016)** – Coordinates a unified government response to significant cyber threats. • **Cybersecurity Information Sharing Act 2015 (CISA)** – Authorizes companies to monitor and implement defensive measures on their own information systems to counter cyber threats. • **FAST Act (2015)** – Allows the Secretary of Energy to direct energy companies to implement specific, short-term cyber attack mitigation technologies following a Grid Security Emergency.	improved security tools, not mitigation measures. • **Sarbanes-Oxley Act (SOX) of 2002 and SEC Statement and Guidance on Public company Cybersecurity Disclosures** provide specific directives and guidance to implement those directives, but these are limited to public companies. • **Executive Order 13800** does not specify access to classified information per se; does not provide directive to private sector to share cyber threats. • **Presidential Policy Directive 41** does not instruct private sector to present a shared and unified response to cyber threats. Applies policies and procedures to incidents where the federal department or agency is victim. • **CISA (2015)** is limited to sharing information and not mitigation efforts that can be applied to the broader critical infrastructure community. • **FAST Act** is limited to the Secretary of Energy and energy companies, and to emergency situations that are unlikely to affect long-term cybersecurity improvements. • **Executive Order 13691** develops more efficient means for gathering clearances but does not specifically share classified information. • **Executive Order 13636** stops short of creating new federal requirements, resources, or authorities to support systemically important critical infrastructure or additional expectations on the private-sector entities that receive it. • **NISPOM** applies specifically to contractor information systems. • **SAFETY Act** only provides liability protection if a company applies for Qualified Anti-Terrorism Technologies designation. • **Homeland Security Act** prioritizes intergovernmental sharing and countering weapons of mass destruction over cyber defense per se.

Existing Authorities	Potential Gaps in Authorities
• **Executive Order 13691: Promoting Private Sector Cybersecurity Information Sharing (2015)** – Directs private companies, nonprofit organizations, executive departments, and agencies to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible. • **Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013)** – Increases the volume, timeliness, and quality of cyber threat information sharing. • **National Industrial Security Program Operating Manual (NISPOM, 2013)** – Protects classified information, and specifically covers classified information systems owned and operated by cleared industry. • **SAFETY ACT (2002)** – Provides incentives for deploying effective anti-terrorism technologies, services, and capabilities. • **Homeland Security Act (2002)** – Section 301 established the DHS Directorate of Science and Technology with a broad mandate to encourage the development of technologies for homeland security, to include establishing a system for transferring homeland security developments to federal, state, and local government and private sector entities.	

CICC Capability
3. **Assess a threat or vulnerability's consequences to broader critical infrastructure sectors**, assist in issuing alerts that can be shared broadly, and share tools to help determine if the identified vulnerability is on a company's system.

Existing Authorities	Potential Gaps in Authorities
• **Executive Order 13920: Securing the Bulk Power System (2020)** – Establishes a Task Force on Federal Energy Infrastructure Procurement Policies that seeks to improve the sharing of risk information and risk management practices to inform such procurement. • **Secure and Trusted Communications Networks Act (2020)** – Requires the Federal Communications Commission to publish a list of products prohibited for use by advanced telecommunications providers for posing an undue national security risk. • **State and Local Government Cybersecurity Act (2019) –** Encourages national cybersecurity watchdogs to share information regarding cybersecurity threats, vulnerabilities, and breaches. Helps bolster all levels of government defense from sophisticated cyberattacks. • **National Cybersecurity Preparedness Consortium Act (NCPCA, 2019) –** Aids the process of preparing for and responding to national, state, and local level risks. Provides private-sector insight into the implications of threats to company systems and validates the impact the threat would have on critical infrastructure systems. • **Presidential Policy Directive 41 (2016) –** Coordinates a unified government response to significant cyber threats. • **Executive Order 13718, Commission on Enhancing National Cybersecurity (2016) –** Established commission within the Department of Commerce to develop recommendations to ensure that cybersecurity is integrated into the Internet of Things and to suggest investments in research and development initiatives that can enhance	• **Executive Order 13920** is focused on federal government efforts, although it must contemplate private sector engagement given that procurement for the bulk power system is predominately a private sector activity. • **Secure and Trusted Communications Networks Act** is focused on telecommunications equipment and the list of prohibited equipment is unlikely to be published before spring of 2021; the FCC has sought not to drive the process of identifying equipment but to seek feedback from industry through the rulemaking process to do so. • **State and Local Government Cybersecurity Act** limited to state and local governments. • **NCPCA** does not specify if government entities can share classified information with private sector; does not provide incentive or direction for private sector to share insight with government entities; is specific to emergency situations; and does not offer a center to analyze threat intelligence. • **State and Local Government Cybersecurity Act** is limited to state and local governments; and does not occur in real- time. • **Presidential Policy Directive 41** does not instruct private sector to present a shared and unified response to cyber threats. • **CISA** encourages sharing and insight into threats to private and public systems but does not provide the tools to help determine if the vulnerability is on a company's system o assistance in developing the alert. • **Executive Order 13718** established a Commission that has now dissolved.

Existing Authorities	Potential Gaps in Authorities
cybersecurity; the Commission issued its final report in 2016, which recommended developing a joint cybersecurity operation program for cyber incident response that may be leveraged to advocate for a similar program. • **FAST Act (2015) –**Allows the Secretary of Energy to direct energy companies to implement specific, short-term cyber attack mitigation technologies following a Grid Security Emergency. • **Executive Order 13636 – Improving Critical Infrastructure Cybersecurity (2013) –** Increases the volume, timeliness, and quality of cyber threat information sharing.	• **FAST Act is** specific to the Secretary of Energy and energy companies; and limited to emergency situations. • **Executive Order 13636** stops short of creating new federal requirements, resources, or authorities to support systemically important critical infrastructure or additional expectations on the private-sector entities that receive it.

CICC Capability
4. **Monitor threat activity on infrastructure systems that could indicate targeting of a particular sector or device/system**, provide sector-specific insight to assess impacts to operations and supply chain, and inform appropriate government or company response.

Existing Authorities	Potential Gaps in Authorities
• **National Cybersecurity Preparedness Consortium Act (NCPCA, 2019) –** Aids the process of preparing for and responding to national, state, and local level risks. Provides private-sector insight into the implications of threats to company systems and validates the impact the threat would have on critical infrastructure systems. • **National Defense Authorization Act (NDAA) of 2019 Section 889 –** Restricts the federal government's direct purchase of certain prohibited telecommunications equipment and from contracting with an entity that uses any such equipment that serves as a substantial or essential component of any system; this has direct ramifications for critical infrastructure participants using telecommunications equipment that contract with the federal government and serves as a mechanism for the Secretary of Defense to	• **NCPCA** does not provide incentive or direction for private sector to share insight and monitor vulnerabilities with government entities; and is not specific to the sector supply chain. • **NDAA Section 889** is limited to entities that contract with the federal government and to telecommunications equipment, although such equipment may be broadly used across critical infrastructure sectors. • **Executive Order 13873** could have served as authority to help federal government assist private sector telecommunications entities in developing threat intelligence, but Department of Commerce has not promulgated final rules to implement this Executive Order. • **SECURE Technology Act is** limited to bug bounty programs to reduce federal government supply chain threats. • **Sarbanes-Oxley Act (SOX) of 2002 and SEC Statement and Guidance on Public company**

Existing Authorities	Potential Gaps in Authorities
monitor threats to critical infrastructure systems that use such equipment. - **Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain (2019) –** Prohibits any acquisition of information and communications technology where a foreign country or national has any interest if the Secretary of Commerce has determined the transaction poses an undue risk of sabotage. - **SECURE Technology Act (2018) –** Aims to reduce federal government supply chain threats. Creates a Federal Acquisition Security Council that determines what types of products pose supply chain security risks to federal government. - **Sarbanes-Oxley Act (SOX) of 2002 and SEC Statement and Guidance on Public company Cybersecurity Disclosures (2018) –** Section 404 of SOX requires public companies to include in their annual reports management's assessment of the effectiveness of the company's internal controls over financial reporting and an auditor's attestation as to the effectiveness of the internal control structure; such internal controls include IT general controls. The SEC's recent Statement and Guidance on these disclosures assists public companies in preparing disclosures about cybersecurity risks and incidents. Advises companies to implement comprehensive policies and procedures to respond to cyber risks and incidents. - **Executive Order 13800 – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017) –** Supports cybersecurity efforts of critical infrastructure entities. Indicates that DHS seeks to improve access to classified information for critical infrastructure owners and operators and improve incident communication and coordination. - **Cybersecurity Information Sharing Act 2015 (CISA) –** Allows information sharing between the U.S. government and technology and management companies. Authorizes	**Cybersecurity Disclosures** is specific to public companies and is focused on a company's having adequate disclosure controls and procedures in place to help ensure that material risks involving breach vulnerabilities are adequately considered. - **Executive Order 13800** functions as an accountability measure and not as a directive for private owners and operators of critical infrastructure to monitor sector threats. - **CISA** authorizes companies to monitor and implement defensive measures, however, it does not instruct companies to do so; CISA also does not provide understanding to assess impacts of a particular to the sector supply chain. - **Executive Order 13691 –** does not provide understanding to assess impacts of a particular threat to the sector supply chain.

Existing Authorities	Potential Gaps in Authorities
companies to monitor and implement defensive measures on their own information systems to counter cyber threats. • **Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing (2015) –** Directs private companies, nonprofit organizations, executive departments, and agencies to share information related to cybersecurity risks and incidents and collaborate to respond in close to real time as possible.	

CICC Capability
5. **Allow the Intelligence Community (IC) to quickly share threats and intelligence with private companies** and enable the private sector to add valuable context to support improved intelligence collection.

Existing Authorities	Potential Gaps in Authorities
• **Executive Order 13920, Securing the Bulk Power System (2020)** – Requires the Department of Energy to mitigate cyber threats to bulk power system. • **Secure and Trusted Communications Networks Act (2020)** – Requires the Federal Communications Commission to develop an information sharing program regarding supply chain security risks with telecommunications providers and their suppliers. • **Cybersecurity Information Sharing Act 2015 (CISA)** – Allows information sharing between the U.S. government and technology and management companies. Authorizes companies to monitor and implement defensive measures on their own information systems to counter cyber threats. • **Executive Order 13691: Promoting Private Sector Cybersecurity Information Sharing (2015)** – Directs private companies, nonprofit organizations, executive departments, and agencies to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.	• **Executive Order 13920** is focused on the bulk power system and it is unclear whether the Department of Energy's request for information regarding participation in information sharing programs that seeks to implement this Executive Order will lead to improvement in participation in the E-ISAC or other positive outcomes for information sharing in this sector. • **Secure and Trusted Communications Networks Act** is focused on the telecommunications sector and it is unclear what the information sharing program will look like beyond the Communications ISAC. • **CISA (2015)** has restrictions on sharing and use. When a company receives a threat indicator or defensive measure from another party, it must comply with any lawful restrictions the sharing entity imposes on sharing or using that information. CISA also fails to provide a complete limitation on liability such that private entities would be fully incentivized to share threat information. • **Executive Order 13691** does not specify the limitations on sharing and if this is restricted to declassified information.

Existing Authorities	Potential Gaps in Authorities
• **Presidential Policy Directive 21 (2013)** – Develops a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time. • **Homeland Security Information Sharing Act (2002)** – Sought to promote information sharing between federal, state, and local governments and directed the President to prescribe Federal Agency procedures for information sharing with these entities, to include handling of classified information.	• **Presidential Policy Directive 21** improves the relationship between private critical infrastructure companies and government regulators to improve cybersecurity efforts. However, it does not specify how information is shared and whether this includes classified information. It also does not explicitly make the private sector an Intelligence Community customer. • **Homeland Security Information Sharing Act** focuses on intergovernmental sharing and does not specifically contemplate sharing with private entities.

Appendix B. Acknowledgements

Working Group Members

J. Rich Baich, Chief Information Security Officer, AIG (Co-Chair)

Richard H. Ledgett, Jr., Senior Visiting Fellow, The MITRE Corporation; Former Deputy Director, National Security Agency (Co-Chair)

William J. Fehrman, President and CEO, Berkshire Hathaway Energy

Dr. Kevin Morley, Manager of Federal Relations, American Water Works Association

Ola Sage, Founder and CEO, CyberRx; Chair, Vistage Worldwide, Inc.**;** Former IT SCC Chair

Michael J. Wallace, Former Vice Chairman and COO, Constellation Energy

Working Group Support

Jeffrey Baumgartner, Senior Advisor, National Security and Resilience, Berkshire Hathaway Energy; NIAC Point of Contact

Sam Chanoski, Former Director, Threat Intelligence, Electricity Information Sharing and Analysis Center (E-ISAC), North American Electric Reliability Corporation (NERC); Former NIAC Point of Contact

Kristina Dorville, Head of Governance and Engagement, AIG; NIAC Point of Contact

Charles Durant, Former Director of National Security Policy and Resiliency Policy Adviser, Berkshire Hathaway Energy; Former NIAC Point of Contact

Frank Honkus, Associate Director, Intelligence Programs and CRISP Manager, E-ISAC, NERC; NIAC Point of Contact

Gibson, Dunn, & Crutcher LLP, legal analysis

Working Group Interviewees

Peter Altabef, Chairman and CEO, Unisys; and National Security Telecommunications Advisory Committee (NSTAC) member

Abigail Bradshaw, Head, Australian Cyber Security Centre (ACSC)

Christopher J. Button, Chief of Staff, Analysis and Resilience Center (ARC)

Kathryn Condello, Senior Director, National Security/Emergency Preparedness, Lumen Technologies; and NSTAC Point of Contact

John Costello, Senior Director and Lead, Task Force Two, Cyberspace Solarium Commission (CSC); and Senior Advisor, Director of CISA

Michael Daly, Chief Technology Officer, Cybersecurity, Special Missions, Raytheon Technologies; and NSTAC Point of Contact

Michael Daniel, President and CEO, Cyber Threat Alliance (CTA)

Scott DePasquale, President and CEO, Analysis and Resilience Center (ARC)

Christopher Demi, Strategic Advisor, Assistant Commandant for Intelligence (CG-2SA), U.S. Coast Guard (USCG)

Alex Gates, Senior Advisor, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy (DOE)

Katherine Gronberg, Vice President, Government Affairs, ForeScout Technologies; and NSTAC Point of Contact

Sharon Halstead, Deputy Senior National Intelligence Officer, Critical Infrastructure, Bureau Intelligence Council, Federal Bureau of Investigation (FBI)

Karl Hanmore, Acting Head, Australian Cyber Security Centre

Jared Hartter, Director, Kansas Intelligence Fusion Center (KIFC)

Col. Travis Howell, Division Chief Current Operations, USCYBERCOM

John C. "Chris" Inglis, Former Deputy Director, National Security Agency; Commissioner, Cyberspace Solarium Commission

Rodney Joffe, Senior Vice President, Security CTO, Neustar, Inc.; NSTAC member

Ilana Johnson, Facility Security Officer, Trust and Safety Manager**,** Neustar, Inc.; NSTAC Point of Contact

Bob Kolasky, Assistant Director, National Risk Management Center (NRMC), CISA

Kathy Kincaid, Chief, Planning Branch, Operational Collaboration Sub-Division, CISA

Ciaran Martin, Former CEO, National Cyber Security Centre (NCSC)

Mark Montgomery, Executive Director, Cyberspace Solarium Commission

Kim Murphy, Maritime Cyber Consultant, U.S. Coast Guard Intelligence, USCG

Tom Patterson, Chief Trust Officer, Unisys; and NSTAC Point of Contact

Johnny Starrunner, Information Sharing and Analysis Unit (ISAU), Office of the Private Sector, Federal Bureau of Investigation (FBI)

Gary Warner, Jr., Director of Research, Center for Cyber Security (Center) of the University of Alabama at Birmingham (UAB); and Director of Threat Intelligence for DarkTower, Queen Associates

Nicole West, Chief Operating Officer, Analysis and Resilience Center (ARC)

Michael Wolk, Team Lead, National Support/Military Registry Task Force, Cyber National Mission Force (CNMF)

Department of Homeland Security Study Support Resources

Rachel Liang, Designated Federal Officer, NIAC

Jessica Eadie, NIAC Secretariat Support

Nexight Group, LLC

Appendix C. References

After Brexit. “Cybersecurity and Brexit.” January 4, 2020. https://afterbrexit.tech/cybersecurity/.

AusCERT. “AusCERT Information Sharing & Analysis Centre (AusISAC).” 2019. https://www.auscert.org.au/static/static_uploads/2019/07/2019_AusCERT_AusISAC_Prospectus_web.pdf

AusCERT. “Incident Management.” Accessed March 19, 2020. https://www.auscert.org.au/services/incident-management/.

AusCERT. “Services.” Accessed March 18, 2020, https://www.auscert.org.au/services/.

Australian Cyber Security Centre. “AISI Members Info.” Accessed March 20, 2020. https://www.cyber.gov.au/acsc/view-all-content/programs/aisi/members-list.

Australian Cyber Security Centre. “Cyber scams during the COVID-19 crisis – ABC Radio Interview.” March 27, 2020. https://www.cyber.gov.au/news/cyber-scams-during-covid-19-crisis-abc-radio-interview.

Australian Cyber Security Centre. “Joint Cyber Security Centres.” Accessed March 19, 2020. https://www.cyber.gov.au/programs/joint-cyber-security-centres.

Australian Security Intelligence Organisation. “What We Do.” Accessed March 20, 2020. https://www.asio.gov.au/what-we-do.html.

Australian Signals Directorate. “Cyber Security.” Accessed March 19, 2020. https://www.asd.gov.au/cyber.

Blinder, Alan. “Lifesaving Forecasts Start Here: Inside the Storm Prediction Center.” *The New York Times*, April 21, 2019. https://www.nytimes.com/2019/04/21/us/storms-weather-oklahoma.html

Brad S. Karp, Paul, Weiss, Rifkind, Wharton & Garrison LLP. “Federal Guidance on the Cybersecurity Information Sharing Act of 2015.” March 3, 2016. https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/

Bruce, Cody James. “Testimony in support of Senate Bill No. 184.” Kansas State Legislature. March 20, 2017. http://kslegislature.net/li_2018/b2017_18/committees/ctte_s_jud_1/documents/testimony/20170309_01.pdf.

Brumfield, Cynthia. “Leader of New NSA Cybersecurity Directorate Outlines Threats, Objectives.” *CSO.* September 5, 2019. https://www.csoonline.com/article/3435142/leader-of-new-nsa-cybersecurity-directorate-outlines-threats-objectives.html.

Business Standard. “Facebook AI deletes ISIS, Al Qaeda-related posts even before it is flagged.” November 29, 2017. https://www.business-standard.com/article/technology/facebook-ai-deletes-isis-al-qaeda-related-posts-even-before-it-is-flagged-117112900236_1.html.

C-Span. “Election Security.” February 13, 2018. https://www.c-span.org/video/?441121-1/hearing-focuses-election-security

Cappucci, Matthew. “NOAA storm-spotting app was suspended after being overrun with false and hateful reports.” *The Washington Post*. July 14, 2020. https://www.washingtonpost.com/weather/2020/07/14/noaa-app-mping-suspended/?hpid=hp_national1-8-12_greatlakes-425pm%3Ahomepage%2Fstory-ans&itid=hp_national1-8-12_greatlakes-425pm%3Ahomepage%2Fstory-ans

CISOMAG. “Australia launches new Joint Cybersecurity Center in Adelaide.” November 27, 2018. https://www.cisomag.com/australia-launches-new-joint-cybersecurity-center-in-adelaide/.

Coats, Daniel R. “Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community.” Before the Senate Select Committee on Intelligence. January 29, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Commission on Enhancing National Cybersecurity (CENC). *Report on Securing and Growing the Digital Economy*. December 2016. https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

Commonwealth of Australia, Home Affairs. “Australia’s 2020 Cyber Security Strategy: A Call for Views.” 2019. https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf.

Corfield, Gareth. “UK-EU infosec data sharing may not be KO’d by Brexit, reckons ENISA bod.” *The Register*. January 25, 2019. https://www.theregister.co.uk/2019/01/25/enisa_steve_purser_interview/.

Corfield, Gareth. “We’re not omnipotent,’ trills National Cyber Security Centre in open-armed pitch to UK biz.” *The Register.* April 24, 2019. https://www.theregister.co.uk/2019/04/24/ncsc_help_for_biz_public_pitch/.

Cyber Exchange. “About the Cyber Exchange.” Accessed March 19, 2020. https://cyberexchange.uk.net/about-us/.

Cyber Threat Alliance “Membership.”. Accessed July 9, 2020. https://www.cyberthreatalliance.org/membership/

Cyber Threat Alliance. “Partnerships.” Accessed July 8, 2020. https://www.cyberthreatalliance.org/partnerships/

Cybersecurity and Infrastructure Agency. “CISA Central.” Accessed January 12, 2021. https://www.cisa.gov/central.

Cybersecurity and Infrastructure Agency. “Information Sharing and Awareness.” Accessed November 25, 2020. https://www.cisa.gov/information-sharing-and-awareness

Cybersecurity and Infrastructure Security Agency. *National Risk Management.* Accessed February 26, 2020. https://www.cisa.gov/national-risk-management.

Das, Debak. “An Indian nuclear power plant suffered a cyberattack. Here’s what you need to know.” *The Washington Post,* November 4, 2019. https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/.

Dekker, Michael. “‘It’s awesome’: OU’s National Weather Center is epicenter of severe weather.” *Tulsa World*. April 28, 2019. https://www.tulsaworld.com/news/state-and-regional/its-awesome-ous-national-weather-center-is-epicenter-of-severe-weather/article_6feba42c-8d44-5bea-b9e3-11bfa0bbc2a6.html.

Edwards, Jane. “Cybercom, National Guard Help States, Local Governments Address Cyber Threat via ‘Cyber 9-Line.’” *Executive Gov.* June 10, 2020. https://www.executivegov.com/2020/06/cybercom-national-guard-help-states-local-governments-address-cyber-threats-via-cyber-9-line/.

Electricity Subsector Coordinating Council. “Information Sheet.” Last revised June 2017. https://www.naseo.org/Data/Sites/1/documents/2017-institute/escc-initiatives-june-2017.pdf

Electronic Privacy Information Center (EPIC) “Equifax Data Breach.”. Accessed October 15, 2020. https://www.epic.org/privacy/data-breach/equifax/.

European Union Agency for Cybersecurity. “NIS Directive.” Accessed March 16, 2020. https://www.enisa.europa.eu/topics/nis-directive/.

The European Union Agency for Network and Information Security (ENISA). *Public Private Partnerships (PPP): Cooperative Models*. November 2017. https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport.

Executive Office of the President. “Presidential Executive Order on Strengthening the Cybersecurity of FDIC. “Cybersecurity Resources.” January 10, 2018. https://www.fdic.gov/regulations/resources/cybersecurity/

Federal Communications Commission. “Communications Security, Reliability, and Interoperability Council VII.” Accessed August 6, 2020. https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii.

Federal Networks and Critical Infrastructure (E.O. 13800).” May 11, 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

Federal Bureau of Investigation. “National Cyber Investigative Joint Task Force.” Accessed March 12, 2020. https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

Federal Reserve. “Supervisory Policy and Guidance Topics.” Accessed August 6, 2020. https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm

Federal Financial Institutions Examination Council. “FFIEC Forms Cybersecurity and Critical Infrastructure Working Group.” June 6, 2013. https://www.ffiec.gov/press/pr060613.htm

Financial Systemic Analysis & Resilience Center. “U.S. Treasuries (UST) Initiative Highlights.” October 23, 2018. https://www.newyorkfed.org/medialibrary/Microsites/tmpg/files/FSARC_TMPG_Presentation.pdf.

Financial Services Information Sharing and Analysis Center. “Subsidiaries.” Accessed May 21, 2020, https://www.fsisac.com/subsidiaries.

Gibson, Dunn & Crutcher LLP. “Analysis of Federal Regulations and Executive Authorities Available to Accelerate or Further Mitigation of Cyber Risks to Private Infrastructure.” *Berkshire Hathaway Energy,* December 12, 2019.

Global Resilience Federation. “2019 Summit Agenda.” Accessed June 19, 2020. https://grf.org/summit/2019/agenda.

Global Resilience Federation. “Build with GRF.” Accessed June 18, 2020. https://grf.org/build.

Global Resilience Federation. “GRF Summit on Security & Third-Party Risk.” Accessed June 19, 2020. https://grf.org/summit/2020/overview.

Global Resilience Federation. “History of the GRF.” Accessed June 18, 2020. https://grf.org/history.

Global Resilience Federation. “Members.” Accessed June 18, 2020. https://grf.org/members.

Global Resilience Federation. “Support from GRF.” Accessed June 18, 2020. https://grf.org/support

Global Resilience Federation. “Xcel Energy Chief Security Officer James Sample Joins Global Resilience Federation Board of Directors.” June 25, 2020. https://grf.org/all-grf-news/2020/6/25/xcel-energy-chief-security-officer-james-sample-joins-global-resilience-federation-board-of-directors

Greenberg, Andy. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” *Wired*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Grid Modernization Laboratory Consortium, U.S. Department of Energy. “About.” Accessed July 30, 2020. https://gmlc.doe.gov/about

Harvard Kennedy School of Government. “Dr. Michael Sulmeyer.” Accessed 25 June 2020. https://www.hks.harvard.edu/about/dr-michael-sulmeyer

HM Government. “Data protection.” Accessed March 17, 2020. https://www.gov.uk/data-protection.

HM Government. *National Cyber Security Strategy 2016-2020*. 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Jared Harterr. “Testimony presented to the Kansas Joint Committee on Information Technology.” Kansas State Legislature. May 3, 2017. http://kslegislature.org/li_2018/b2017_18/committees/ctte_jt_it_1/documents/testimony/20170503_03.pdf.

JPMorgan Chase. “Identifying Cyber Threats With FSARC.” October 9, 2018. https://www.jpmorgan.com/commercial-banking/insights/cyber-threats-fsarc.

Kansas Legislative Research Department. “Minutes of the Joint Committee on Kansas Security.” December 12, 2018. http://www.kslegislature.org/li_2018/b2017_18/committees/ctte_jt_ks_security_1/documents/minutes/20181212.pdf.

Kansas State Attorney General's Office. "Kansas Intelligence Fusion Center." Accessed March 18, 2020. https://ag.ks.gov/about-the-office/affiliated-orgs/kansas-intelligence-fusion-center.

King's College London. "UK Active Cyber Defense." January 2019. https://www.kcl.ac.uk/policy-institute/assets/uk-active-cyber-defence.pdf.

Lazzarotti, Joseph J. "New York SHIELD Act FAQs." *The National Law Review,* March 11, 2020. https://www.natlawreview.com/article/new-york-shield-act-faqs

Legal Information Institute Cornell Law School. "U.S. Code: Title 10. Armed Forces." Accessed 30 July 2020. https://www.law.cornell.edu/uscode/text/10

Legal Information Institute Cornell Law School. "U.S. Code: Title 50. War and National Defense." Accessed 30 July 2020. https://www.law.cornell.edu/uscode/text/50

Levy, Ian. "Active Cyber Defense – tackling cyber attacks on the UK." *National Cyber Security Centre.* November 1, 2016. https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk.

LinkedIn. "Financial Systemic Analysis and Resilience Center." Accessed May 22, 2020. https://www.linkedin.com/company/fsarc/about/.

LinkedIn. "Global Resilience Federation." Accessed June 19, 2020. https://www.linkedin.com/company/globalresiliencefederation/about/.

Mayo, Josh. "Trump Signs SECURE Technology Act into Law." *Meritalk.* December 24, 2018. https://www.meritalk.com/articles/trump-signs-secure-technology-act-into-law/

The MITRE Corporation. "National Cybersecurity FFRDC." Accessed June 17, 2020. https://www.mitre.org/publications/all/national-cybersecurity-ffrdc.

National Council of ISACs. "Member ISACs." Accessed January 12, 2021. https://www.isao.org/information-sharing-group/sector/communications-isac/.

National Cyber Security Centre. "Active Cyber Defense (ACD) – The Second Year." July 16, 2019. https://www.ncsc.gov.uk/report/active-cyber-defence-report-2019.

National Cyber Security Centre. "The NCSC defends nation against more than 600 cyber attacks." October 23, 2019. https://www.ncsc.gov.uk/news/ncsc-defends-nation-against-more-than-600-cyber-attacks.

National Cybersecurity and Communications Integration Center. *NCCIC Year in Review 2017: Operation Cyber Guardian*. Accessed February 27, 2020. https://www.us-cert.gov/sites/default/files/publications/NCCIC_Year_in_Review_2017_Final.pdf.

National Infrastructure Advisory Council (NIAC). *A Framework for Establishing Critical Infrastructure Resilience Goals.* 2010. https://www.cisa.gov/sites/default/files/publications/niac-framework-establishing-resilience-goals-final-report-10-19-10-508.pdf.

National Infrastructure Advisory Council (NIAC). *Clarifications on Executive Collaboration for the Nation's Strategic Infrastructure: Responses to National Security Council Questions.* 2015. https://www.cisa.gov/sites/default/files/publications/niac-slidedeck-siec-responses-nsc-qbm-12-01-15-508.pdf.

National Infrastructure Advisory Council (NIAC). *Convergence of Physical and Cyber Technologies and Related Security Management Challenges*. 2007. https://www.cisa.gov/sites/default/files/publications/niac-physical-cyber-final-report-01-16-07-508.pdf.

National Infrastructure Advisory Council (NIAC). *Critical Infrastructure Partnership Strategic Assessment*. 2008. https://www.cisa.gov/sites/default/files/publications/niac-ci-partnership-assessment-final-report-10-14-08-508.pdf.

National Infrastructure Advisory Council (NIAC). *Critical Infrastructure Resilience Final Report and Recommendations*. 2009. https://www.cisa.gov/sites/default/files/publications/niac-critical-infrastructure-resilience-final-report-09-08-09-508.pdf.

National Infrastructure Advisory Council (NIAC). *Cross Sector Interdependencies and Risk Assessment Guidance*. 2004. https://www.cisa.gov/sites/default/files/publications/niac-interdependencies-risk-assess-final-report-01-13-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Evaluation and Enhancement of Information Sharing and Analysis*. 2004. https://www.cisa.gov/sites/default/files/publications/niac-eval-enhance-info-sharing-final-report-07-13-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Executive Collaboration for the Nation's Strategic Infrastructure*. 2015. https://www.cisa.gov/sites/default/files/publications/niac-executive-collaboration-final-report-508.pdf.

National Infrastructure Advisory Council (NIAC). *Framework for Dealing with Disasters and Related Interdependencies*. 2009. https://www.cisa.gov/sites/default/files/publications/niac-framework-dealing-disasters-final-report-07-14-09-508.pdf.

National Infrastructure Advisory Council (NIAC). *Future Focus Study: Strengthening the NIAC Study Process*. 2017. https://www.cisa.gov/sites/default/files/publications/niac-future-focus-study-powerpoint-05-08-17-508.pdf.

National Infrastructure Advisory Council (NIAC). *Hardening the Internet*. 2004. https://www.cisa.gov/sites/default/files/publications/niac-hardening-internet-final-report-10-12-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Implementation of EO 13636 and PPD-21.* 2013. https://www.cisa.gov/sites/default/files/publications/niac-eo-ppd-implem-final-report-11-21-13-508.pdf.

National Infrastructure Advisory Council (NIAC). *The Insider Threat to Critical Infrastructures*. 2008. https://www.cisa.gov/sites/default/files/publications/niac-insider-threat-final-report-04-08-08-508.pdf.

National Infrastructure Advisory Council (NIAC). *Intelligence Information Sharing Report*. 2012. https://www.cisa.gov/sites/default/files/publications/niac-intel-info-sharing-final-report-01-10-12-508.pdf.

National Infrastructure Advisory Council (NIAC). *Optimization of Resources for Mitigating Infrastructure Disruptions.* 2010. https://www.cisa.gov/sites/default/files/publications/niac-optimization-resources-final-report-10-19-10-508.pdf.

National Infrastructure Advisory Council (NIAC). *Prioritizing Cyber Vulnerabilities*. 2004. https://www.cisa.gov/sites/default/files/publications/niac-cyber-vulnerabilties-final-report-10-12-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Public-Private Sector Intelligence Coordination*. 2006. https://www.cisa.gov/sites/default/files/publications/niac-intelligence-coordination-final-report-07-11-06-508.pdf.

National Infrastructure Advisory Council (NIAC). *Risk Management Approaches to Protection.* 2005. https://www.cisa.gov/sites/default/files/publications/niac-risk-management-final-report-10-11-05-508.pdf.

National Infrastructure Advisory Council (NIAC). *Sector Partnership Model Implementation*. 2005. https://www.cisa.gov/sites/default/files/publications/niac-sector-partnership-implem-final-report-10-11-05-508.pdf.

National Infrastructure Advisory Council (NIAC). *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*. 2017. https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf.

National Infrastructure Advisory Council (NIAC). *Strengthening Regional Resilience*. 2013. https://www.cisa.gov/sites/default/files/publications/niac-regional-resilience-final-report-11-21-13-508.pdf.

National Infrastructure Advisory Council (NIAC). *Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation*. 2018. https://www.cisa.gov/sites/default/files/publications/NIAC%20Catastrophic%20Power%20Outage%20Study_FINAL.pdf.

National Infrastructure Advisory Council (NIAC). *Vulnerability Disclosure Framework.* 2004. https://www.cisa.gov/sites/default/files/publications/niac-vulnerability-framework-final-report-01-13-04-508.pdf.

National Security Agency Press Room. "NSA Names Anne Neuberger New Deputy National Manager." October 3, 2019. https://www.nsa.gov/news-features/press-room/Article/1977307/nsa-names-anne-neuberger-new-deputy-national-manager/.

National Security Agency, Central Security Service, Cybersecurity Directorate Engagements. "Strengthening the Front Line: NSA Launches New Cybersecurity Directorate." October 1, 2019, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/1973871/strengthening-the-front-line-nsa-launches-new-cybersecurity-directorate/.

National Security Telecommunications Advisory Committee (NSTAC). *NSTAC Report to the President on a Cybersecurity Moonshot*. November 2018. https://www.cisa.gov/sites/default/files/publications/NSTAC_CyberMoonshotReport_508c.pdf.

National Vulnerability Database, News. "2019 in Review." Accessed November 23, 2020. https://nvd.nist.gov/General/News/2019-in-Review

National Weather Center. "National Weather Center Partners." Accessed July 10, 2020. https://www.ou.edu/nwc/partners.

Newman, Lily Hay. "NSA Cybersecurity Boss Anne Neuberger on What Keeps Her Up at Night." *Wired.* November 8, 2019. https://www.wired.com/story/anne-neuberger-national-security-agency-wired25/.

Newsroom, U.S. Senator Gary Peters (D-MI). "Senate Passes Peters Bill to Strengthen Cybersecurity Coordination with State and Local Governments." November 22, 2019. https://www.peters.senate.gov/newsroom/press-releases/senate-passes-peters-bill-to-strengthen-cybersecurity-coordination-with-state-and-local-governments#:~:text=The%20State%20and%20Local%20Government,increasingly%20targeted%20by%20bad%20actors.

NOAA National Severe Storms Laboratory. "mPing: crowdsourcing weather reports." Accessed July 15, 2020. https://mping.nssl.noaa.gov/.

North American Electric Reliability Corporation. "Critical Infrastructure Protection Committee (CIPC)." Accessed July 27, 2020. https://www.nerc.com/comm/CIPC/Pages/default.aspx

Oberly, David J. "Ohio's Data Protection Act." July 1, 2019. https://www.ohiobar.org/member-tools-benefits/practice-resources/practice-library-search/practice-library/2019-ohio-lawyer/ohios-data-protection-act/

Palmer, Danny. "On data protection, the UK says it will go it alone. It probably won't." *ZDNet*. February 14, 2020. https://www.zdnet.com/article/on-data-protection-the-uk-says-it-will-go-it-alone-it-probably-wont/.

Payment Card Industry Security Standards Council. *Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1* (Jul. 2019). https://www.pcisecuritystandards.org/pdfs/Mapping-PCI-DSS-to-NIST-Framework.pdf?agreement=true&time=1573030536849.

PR Newswire. "Global Resilience Federation Launched to Coordinate Cross-Sector information Sharing for ISACs, ISAOs, CERTs, and other Communities." May 2, 2017. https://www.prnewswire.com/news-releases/global-resilience-federation-launched-to-coordinate-cross-sector-information-sharing-for-isacs-isaos-certs-and-other-communities-300448242.html.

Office of the Director of National Intelligence. "History." Accessed May 27, 2020. https://www.intelligence.gov/mission#history.

Office of the Director of National Intelligence. "NCTC: Who we are." Accessed March 12, 2020. https://www.dni.gov/index.php/nctc-who-we-are.

Polit, Kate. "Cyber Threat Alliance, Center for Internet Security Partnership Agreement." Accessed July 9, 2020. https://www.meritalk.com/articles/cyber-threat-alliance-center-for-internet-security-ink-partnership-agreement/

President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures*. October 1997. https://www.hsdl.org/?abstract&did=986.

Rohan, Alicia. “New partnership between Facebook, UAB to help fight online drug sales.” The University of Alabama at Birmingham. November 13, 2018. https://www.uab.edu/news/research/item/9955-new-partnership-between-facebook-uab-to-help-fight-online-drug-sales.

Sabbagh, Dan. “UK to launch specialist cyber force able to target terror groups.” *The Guardian*. February 27, 2020. https://www.theguardian.com/technology/2020/feb/27/uk-to-launch-specialist-cyber-force-able-to-target-terror-groups.

Segrest, Doug. “UAB forensics team DarkTower leaves criminals with nowhere to hide*.” Alabama News Center*. November 15, 2019. https://alabamanewscenter.com/2019/11/15/uab-forensics-team-darktower-leaves-criminals-with-nowhere-to-hide/

Sengupta, Kim. “UK is nearly ready to launch force to hit hostile countries with cyberattacks.” *The Independent*. January 10, 2020. https://www.independent.co.uk/news/uk/home-news/cyber-warfare-security-force-iran-crisis-ministry-of-defence-a9278591.html.

Sheth, Sonam. “Hackers breached a US nuclear power plant’s network, and it could be a ‘big danger.’” *Business Insider*, June 29, 2017. https://www.businessinsider.com/nuclear-power-plant-breached-cyberattack-2017-6.

Shonesy, Katherine. “UAB to serve on the council to support a new federally funded cybersecurity center.” The University of Alabama at Birmingham. October 23, 2014. https://www.uab.edu/news/campus/item/5451-uab-to-serve-on-council-to-support-a-new-federally-funded-cybersecurity-center.

State of California Department of Justice. “California Consumer Privacy Act (CCPA).” Accessed August 3, 2020. https://oag.ca.gov/privacy/ccpa#:~:text=The%20California%20Consumer%20Privacy%20Act,rights%20for%20California%20consumers%2C%20including%3A&text=The%20right%20to%20delete%20personal,them%20(with%20some%20exceptions)%3B

Tech UK. “Cyber Growth Partnership.” Accessed March 19, 2020. https://www.techuk.org/cyber-growth-partnership.

Timmons, John and Gabel, Dr. Detlev. “Proposal on the Application of the NIS Regulations post-Brexit.” *White & Case*. October 23, 2019. https://www.whitecase.com/publications/alert/proposal-application-nis-regulations-post-brexit.

U.S. Coast Guard. *Cyber Strategy*. June 2015. https://www.uscg.mil/Portals/0/Strategy/Cyber%20Strategy.pdf.

U.S. Department of Defense, U.S. Cyber Command. “About.” Accessed June 26, 2020. https://www.cybercom.mil/About/Mission-and-Vision/.

U.S. Department of Defense, U.S. Cyber Command. “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command.” April 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

U.S. Department of Defense, U.S. Cyber Command. “Mission.” Accessed June 26, 2020. https://www.cybercom.mil/About/Mission-and-Vision/.

U.S. Cyberspace Solarium Commission. *Cyberspace Solarium Commission Final Report*. March 2020. https://www.solarium.gov/report.

U.S. Department of Defense, Cyber Crime Center (DC3). “DIB Cybersecurity (DCISE).” November 25, 2020. https://www.dc3.mil/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/

U.S. Department of Defense, Defense Security Service. “Industrial Security letter.” July 2, 2013. https://fas.org/sgp/library/nispom/isl2013-05.pdf

U.S. Department of Defense, Joint Chiefs of Staff. “Joint Publication 3-12, Cyberspace Operations.” June 8, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

U.S. Department of Defense, U.S. Army Cyber Command. “DOD Fact Sheet: Cyber Mission Force.” February 10, 2020. https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/.

U.S. Department of Defense, U.S. Cyber Command. "Cyber 9-Line' Improves Cybersecurity and Enables Election Integrity." June 9, 2020. https://www.cybercom.mil/Media/News/Article/2213264/cyber-9-line-improves-cybersecurity-and-enables-election-integrity/

U.S. Department of Homeland Security. "Critical Infrastructure Partnership Advisory Council Frequently Asked Questions." January 2018. https://www.cisa.gov/cipac-frequently-asked-questions.

U.S. Department of Homeland Security. "Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Last Revised February 27, 2019. https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure.

U.S. Department of Homeland Security. "Fact Sheet EO 13636 and PPD 21." Accessed July 21, 2020. https://www.cisa.gov/sites/default/files/publications/eo-13636-ppd-21-fact-sheet-508.pdf.

U.S. Department of Homeland Security. "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force." https://www.dhs.gov/cisa/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force.

U.S. Department of Homeland Security. "National Cybersecurity and Communications Integration Center (NCCIC)." Accessed February 27, 2020, https://www.dhs.gov/taxonomy/term/946/all/feed.

U.S. Department of Homeland Security. "National Infrastructure Protection Plan." Last revised November 21, 2018. https://www.cisa.gov/national-infrastructure-protection-plan.

U.S. Department of Homeland Security. "SAFETY Act." Updated July 16, 2020. https://www.safetyact.gov/lit/hfpdf/Safety_Act_Legislation.

U.S. Department of Transportation. "The Fixing America's Surface Transportation Act or 'FAST ACT.'" Accessed August 3, 2020. https://www.transportation.gov/fastact

U.S. Government Accountability Office. "DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force.". March 2019. https://www.gao.gov/assets/700/697268.pdf.

U.S. Government Accountability Office. "Nuclear Supply Chain: NNSA Should Notify Congress of its Recommendations to Improve the Enhanced Procurement Authority." August 8, 2019. https://www.gao.gov/assets/710/700794.pdf.

U.S. House of Representatives, Committee on Oversight and Government Reform. *The Equifax Data Breach: Majority Staff Report, 115th Congress.* December 2018, accessed October 15, 2020. https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.

U.S. House of Representatives. "H.R. 3162 - Uniting America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT (Act of 2001)." Accessed November 25, 2020. https://www.congress.gov/bill/107th-congress/house-bill/3162/text.

U.S. House of Representatives. "H.R. 3763 - Sarbanes-Oxley Act of 2002." Accessed November 25, 2020. https://www.congress.gov/bill/107th-congress/house-bill/3763.

U.S. House of Representatives. "H.R. 4718 – Computer Fraud and Abuse Act of 1986." Accessed July 29, 2020. https://www.congress.gov/bill/99th-congress/house-bill/4718.

U.S. House of Representatives. "H.R. 4998 – Secure and Trusted Communications Networks Act of 2019." Accessed November 25, 2020. https://www.congress.gov/bill/116th-congress/house-bill/4998/all-info.

U.S. House of Representatives. "H.R. 5005 - Homeland Security Act of 2002." Accessed November 25, 2020. https://www.congress.gov/bill/107th-congress/house-bill/5005.

U.S. House of Representatives. *John S. McCain National Defense Authorization Act for Fiscal Year 2019*. H.R. 5515. 115th Congress. https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

U.S. House of Representatives. “National Defense Authorization Act for Fiscal Year 2019.” May 15, 2018. https://www.congress.gov/115/crpt/hrpt676/CRPT-115hrpt676.pdf

U.S. House of Representatives. “S.333-National Cybersecurity Preparedness Consortium Act of 2019.” December 4, 2019. https://www.congress.gov/bill/116th-congress/senate-bill/333.

U.S. House of Representatives “S. 3207-Cybersecurity State Coordinator Act of 2020.”. March 31, 2020. https://congress.gov/bill/116th-congress/senate-bill/3207.

U.S. House of Representatives. “S.754 – To Improve Cybersecurity in the United States Through Enhanced sharing of Information about Cybersecurity Threats and for other Purposes.” Accessed July 28, 2020. https://www.congress.gov/bill/114th-congress/senate-bill/754.

U.S. Securities and Exchange Commission. “SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures.” February 21, 2018. https://www.sec.gov/news/press-release/2018-22.

U.S. Senate, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs. *How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach: Staff Report.* Accessed October 15, 2020. https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf.

United States Coast Guard Intelligence. “Our Organization.” Accessed May 27, 2020. https://www.dco.uscg.mil/Our-Organization/Intelligence-CG-2/.

The University of Alabama at Birmingham. “Gary Warner.” Accessed June 17, 2020. https://www.uab.edu/news/experts/all-experts-category/item/1114-warner-gary.

The University of Alabama at Birmingham, Center for Cyber Security. “Governance.” Accessed June 17, 2020. https://www.uab.edu/cas/thecenter/20-members/60-members.

The University of Alabama at Birmingham, Center for Cyber Security. “Information Assurance.” Accessed June 17, 2020. https://www.uab.edu/cas/thecenter/core-areas/information-assurance.

The University of Alabama at Birmingham, Center for Cyber Security. “Information Intelligence and Analytics.” Accessed June 17, 2020. https://www.uab.edu/cas/thecenter/core-areas/information-intelligence-analytics.

The University of Alabama at Birmingham, Center for Cyber Security. “Physical and Digital Forensics.” Accessed June 17, 2020. https://www.uab.edu/cas/thecenter/core-areas/physical-digital-forensics.

The University of Alabama at Birmingham. “SECRETLab.” Accessed June 17, 2020. https://www.uab.edu/cas/computerscience/research/research-labs/secretlab.

The University of Alabama at Birmingham, Center for Cyber Security. “Research and Core Areas.” Accessed June 17, 2020. https://www.uab.edu/cas/thecenter/core-areas.

University of North Carolina Charlotte. “Tom Bartolomeo.” Accessed March 5, 2020. https://cybersecuritysymposium.uncc.edu/speaker/tom-bartolomeo.

Vavra, Shannon. “NSA: ‘We Know We Need to do Some Work on Declassifying Threat Intel.’” *Cyberscoop.* October 24, 2019. https://www.cyberscoop.com/anne-neuberger-nsa-threat-intelligence-cyber-talks-2019/.

Vavra, Shannon. “The NSA is Piloting a Secure DNS Service for the Defense Industrial Base.” *Cyberscoop*. June 18, 2020. https://www.cyberscoop.com/nsa-secure-dns-service-pilot-defense-industrial-base/.

Walton, Robert. “First cyberattack on solar, wind assets revealed widespread grid weaknesses, analysts say.” *Utility Dive,* November 4, 2019. https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/566505/.

The White House. "Executive Order on Securing the Information and Communications Technology and Services Supply Chain." May 15, 2019. https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

The White House. "Executive Order on Securing the United States Bulk-Power System." May 1, 2020. https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/.

The White House. "Executive Order – Commission on Enhancing National Cybersecurity." February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity

The White House. "Executive Order – Promoting Private Sector Cybersecurity Information Sharing." February 13, 2015. https://www.archives.gov/files/isoo/policy-documents/eo-13691.pdf

The White House. "Presidential Policy Directive – United States Cyber Incident Coordination." July 26,2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

The White House. "The Comprehensive National Cybersecurity Initiative." 2008. https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf

Wired. "NSA Director of Cybersecurity Anne Neuberger in Conversation with Garrett Graff." November 8, 2019. https://www.wired.com/video/watch/nsa-director-of-cybersecurity-anne-neuberger-in-conversation-with-garrett-graff.

Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *Wired*, March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Zucker, Rachel. "NSA Launches Cybersecurity Directorate to Combat Cyber Attacks on Government and Private Sector Systems." *Lexology.* October 22, 2019. https://www.lexology.com/library/detail.aspx?g=f886ec9e-3027-439d-807b-44d861278b78.