August 30, 2023

Recommendations with corresponding justifications to policy and regulatory decision-makers/institutions for cross-sector regulatory standards[1]

Linton Wells II
Kathryn Blackmond Laskey
Center for Resilient and Sustainable Communities
George Mason University

Introduction

The purpose of this report is to provide recommendations, along with corresponding justifications, to policy and regulatory decision-makers and institutions for cross-sector regulatory standards to address and mitigate the risks of cascading infrastructure failures. A companion report [1] focuses on elements of five infrastructure sectors that are closely related to Department of Defense (DoD) planning and operations: energy, communications, transportation, information technology, and emergency services. That report reviews existing policy and regulatory standards for disaster response and resilience and then briefly describes the nature and importance of the cross-sector interactions in these areas and the components of resilience. It also examines capabilities that are available, and their limitations, for enabling coordinated, cross-sector planning and operation of critical cyber and physical infrastructures.

There is a wealth of available high-level guidance on infrastructure resilience and cybersecurity, much of which emphasizes the need for cross-sector planning and collaboration. This guidance is useful and important but turning it into effective practice is hard, especially in county and city governments, and at field activities, which may not be fully resourced. The present document provides recommendations for regulatory standards and procedural changes that can address these challenges.

The terms resilience and resiliency are used without definition in many publications, including those synopsized below. They are synonymous, and the standard dictionary definition is the ability to withstand and recover from difficulty. This is the definition of resilience used by many government publications (e.g., [2]; [3]). In 2013, a White House Presidential Policy Directive added two additional capabilities, defining resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions" [4]. The four capabilities – prepare, withstand, recover, adapt – have been incorporated into the definitions in several recent government publications (e.g., [5, p. 75]; [6, pp. 3–1]), as well as archival publications (e.g.,

[1] [1] This paper was partially funded by a grant from the U.S. Defense Department's Strategic Environmental Research and Development Program (RC20-C1-1138): Severe Impact Resilience: Framework for Adaptive Compound Threats. These views are the authors' own and do not reflect the position of the U.S. government.

[7]; [8]). This is the definition used here. The ability to adapt to the post-disruption "new normal" is an important distinction from just returning to a pre-disruption status quo.

High-Level Guidance

Reference [1] notes over 200 policy, strategy, planning and operational guidance documents (see, e.g., the DoD Cybersecurity Policy Chart [9], included as an appendix to [1]). Based on this review, the present paper focuses on five high-level strategy documents: the Cybersecurity and Infrastructure Security Agency (CISA) Strategic Plan 2023-2025 [10], the CISA Cybersecurity Strategic Plan 2024-2024 [11], the National Cybersecurity Strategy [12], the National Cybersecurity Strategy Implementation Plan [13], and the CISA Cross-Sector Cybersecurity Performance Goals [14]. We also considered applicable parts of the sector-specific plans for: Energy (focused on electricity) [15], communications (terrestrial, satellite, and wireless systems with many interdependencies) [16], transportation (focused on road transport for infrastructure repair) [17], Information Technology (for cyber threats and vulnerabilities) [18], and Emergency Services (emergency management) [19]. These were examined in more detail in [1]. The review has been supplemented by discussions with leaders at the White House Office of the National Cyber Director (ONCD), CISA, the Office of the Secretary of Defense (OSD), county and city government officials, and private sector individuals.

CISA Strategic Plan 2023-2025

CISA's Strategic Plan [10] is broader than cyber. It lays out four ambitious goals to address risks to all parts of our nation's infrastructure: (1) Cyber-defense; (2) Risk reduction and resilience; (3) Operational collaboration; and (4) Agency unification. Collectively they include 19 objectives. The first goal, cyber-defense, emphasizes the defense and resilience of cyberspace, to be achieved through enhancing the ability of federal systems to withstand cyberattacks, improving the ability to detect cyber threats, disclosing and mitigating cyber vulnerabilities, and driving the cyberspace ecosystem toward security-by-default. The second goal, risk reduction and resilience, emphasizes expanding visibility of risks to infrastructure, systems and networks, advancing risk analytic capabilities and methodologies, improving risk mitigation guidance and impact, building stakeholder capacity in security and resilience, increasing CISA's ability to respond to threats and incidents, and supporting risk management for election infrastructure. The third goal, operational collaboration, is devoted to strengthening whole-of-nation collaboration and information sharing. While cross-sector collaboration is important to achieving all four goals set forth in the Strategic Plan, this third goal speaks directly to the essential need for collaboration and information sharing among all stakeholders, both government and private partners, and improving stakeholder access to and use of appropriate CISA programs, products, and services. The fourth goal, agency unification, aims to achieve "One CISA" unified through integrated functions, capabilities, and workforce.

CISA Cybersecurity Strategic Plan 2024-2026

CISA's Cybersecurity Strategic Plan [11] aligns with the 2023 National Cybersecurity Strategy (discussed below). It describes how CISA will execute its cybersecurity mission and advance its cybersecurity capabilities. CISA's overall mission, its North Star, is:

> *Defending the systems and assets that constitute our critical infrastructure is vital to our national security, public safety, and economic prosperity ... We aim to operationalize an enduring and effective model of collaborative defense that equitably distributes risk and responsibility and delivers a foundational level of security and resilience for our digital ecosystem* [11, p. 3].

CISA's cybersecurity mission, which is critical to its overall mission, is addressed through three goals: (1) Address immediate threats; (2) Harden the terrain; and (3) Drive security at scale. All three of these goals involve cross-sector collaboration. The first goal involves gaining an understanding of the immediate threats facing all critical infrastructure sectors and supporting partners across sectors in addressing these threats. The second goal requires working to promote adoption of strong security practices across critical infrastructure sectors and measure progress against this goal across sectors. The third goal involves asking technology providers to build security into the foundation of products across their lifecycle, fostering radical transparency in security practices, and developing a diverse and security-aware workforce across all sectors.

National Cybersecurity Strategy

The White House's National Cybersecurity Strategy [12] envisions a grand ambition for values-driven development of the nation's digital ecosystem:

> *We are building a smart grid, powered by distributed renewable electricity and balanced with intelligent systems, that promises a bright and resilient future of energy abundance. We envision a maturing "Internet of Things" (IoT), comprising everything from consumer goods to digitized industrial controls to constellations of satellites, that will increase efficiency and safety while providing game-changing insights into our environment and economy. We are laying the foundations for real-time global collaboration leveraging vast amounts of data and computing power that will unlock scientific discoveries and other public goods of which we cannot yet conceive* [12, p. 1].

The strategy makes two fundamental shifts in roles, responsibilities, and resource allocation: (1) Responsibility to defend cyberspace must shift from individual citizens and small organizations to the most capable and best-positioned actors; and (2) Incentives must be realigned to favor long-term investments in security and resilience. The strategy rests on five pillars: (1) Defend critical infrastructure; (2) Disrupt and dismantle threat actors; (3) Shape market forces to drive security and resilience; (4) invest in a resilient future; and (5) Forge international partnerships to pursue shared goals. Again, because cybersecurity pervades all of today's infrastructure, achieving these goals requires working across infrastructure sectors.

The shift in responsibility for security, away from small actors to those most capable of bearing the burden is a fundamental change in the cybersecurity ecosystem. It is clear that the unfettered market alone has not led to broad adoption of best practices in cybersecurity, and policy initiatives are needed to bring about this shift. The Cybersecurity Strategy seeks to incentivize security through Federal purchasing power, liability law, and a federal cyber insurance backstop. Grants and other incentives will drive investments in secure critical infrastructure, and vendors who sell to the Federal government will be required to follow the best security practices. Liability laws will be changed so that products and services that fail to follow cybersecurity best practices can be held liable for the damage caused by their products.

National Cybersecurity Strategy Implementation Plan

The White House's National Cybersecurity Strategy Implementation Plan [13] lays out a roadmap for coordinated action by government and society to implement the National Cybersecurity Strategy [12]. For each pillar of the National Cybersecurity Strategy, and each strategic objective under the pillar, the implementation plan lays out a set of initiatives that contribute to the objective. Each is assigned a responsible agency and contributing agencies, and a target completion date between Q4 FY23 and Q4 FY 25.

CISA Cross-Sector Cybersecurity Performance Goals

The CISA Cross-Sector Cybersecurity Performance Goals [14] is "a prioritized subset of information technology (IT) and operational technology (OT) cybersecurity practices that critical infrastructure owners and operators can implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques." These are voluntary goals "intended to help establish a common set of fundamental cybersecurity practices for critical infrastructure, and especially help small- and medium-sized organizations kickstart their cybersecurity efforts."

Discussion

The high-level guidance is comprehensive, and well thought out, but implementing it is hard, especially for understaffed local agencies and small and medium-sized enterprises (SMEs) that must sort through the reams of guidance and dig out what applies to them. Senior officials repeatedly state that the guidance is designed to allow local officials and infrastructure owners/operators to implement in ways that best suit their own situations. This decentralization is admirable, but a frequently offered phrase from short-staffed emergency responders was something like, "We're running like gerbils on treadmills and don't have time to address issues outside of our specific areas."

The market and legal incentives set forth in the National Cybersecurity Strategy will, if effectively implemented, help to take some of the load off SMEs. If products and services are more secure out of the box, then securing SMEs is likely to become less taxing. But this will take time, and the strategy of shaping market forces and shifting liability is unlikely to remove the burden entirely. For example, there will likely remain large quantities of guidance that must be sorted through and tailored to local needs. Even when the guidance is parsed to local needs, and understood, challenges to individuals and SMEs to implement their parts will undoubtedly remain. Consequently, an urgent need remains to keep some levels of support for these small actors in improving their cybersecurity practices. This is especially important given the rapid proliferation of IoT and connected devices in all sectors of society.

Recommendations

As noted in reference [1], there is less need for new policy now than for effective implementation. To this end, whatever standards may be chosen, solutions to complex society-wide challenges cannot be achieved with technology alone, but require integration among *People, Organizations, Processes, Technology, and Resources*. If the recommendations offered below are to be effectively implemented, they must be supported by appropriate and thorough training; processes must be defined and developed that enable the recommendations to be implemented; authority and responsibility must be assigned to carrying out the recommendations; management must be committed to implementation; and success criteria must be defined and measured. Most importantly, we recognize that regulations and directives often come as unfunded mandates, and this creates major impediments for effective implementation. Therefore, it is essential that these recommendations are adequately funded. An important example of how this can be done is the no-cost cybersecurity incident response (IR) training that CISA has developed for government employees and contractors across Federal, State, Local, Tribal, and Territorial government [20]. It is also open to educational and critical infrastructure partners.

The National Cybersecurity Strategy's goal of shifting more of the burden to the most capable actors and taking some of the burden off SMEs is admirable, but it is essential to keep strengthening local abilities to execute during the transition. For example, given the present complexity of the guidance, larger cities/counties with strong state organizations are more able to execute it effectively (Northern Virginia is an example). At the same time, smaller organizations / municipalities are likely to need support for the foreseeable future to be able to tailor and implement the available guidance. Some ideas for addressing this issue include forming consortia of local SMEs to share resources and expertise; using artificial intelligence to support the process of tailoring guidance to local needs; and finding ways to make security practices simpler and less burdensome for end users, for example by adjusting the required standards based on the level of risk and the ability of the regulated organization to implement them. Several recommendations related to these ideas follow.

Consortia of local organizations. Consortia of local SMEs, plus other entities with similar missions and situations, could band together as a group to sort through the guidance and develop tailored best practices that suit the needs of consortium members. This often is done today with emergency managers, both within jurisdictions and among adjacent jurisdictions. Consortia can also pool resources, as in sharing the expertise of security staffs. The National Cyber Incident Response Plan (NCIRP) [21] is designed to "bolster coordination at the local level."

R1. **Recommendation:** *Formulate policies and guidance that incentivize the formation of consortia of similar organizations (public and private) to develop and implement common best cybersecurity practices, especially those involving cross-sector interdependencies, based on members' specific situations and needs.*

R2. **Recommendation:** *Explore innovative funding opportunities, such as Other Transaction Authorities (OTAs) within DoD and other eligible agencies to facilitate the resourcing of such consortia.*

R3. **Recommendation:** *Incentivize research to examine the barriers and challenges to information sharing and collaboration between public and private entities, especially* *across sectors, before, during, and after disasters. Such research should be directed toward identifying ways to enhance sharing without compromising sensitive information.*

Artificial Intelligence. Recent advances in artificial intelligence (AI) could be leveraged to support the development of systems that can parse existing cybersecurity guidance and tailor it to local needs and resources.

R4. **Recommendation:** *Incentivize research to investigate the feasibility of using AI language models focused on cybersecurity and cross-sector guidance, as well as chatbots or similar technology, to help local users sort through guidance documents and recommend specific approaches tailored to local needs and resources.*

Individual self-defense: The major policy shift in the National Cybersecurity Strategy [12] to which cyberspace defense responsibilities "from individual citizens and small organizations to the most capable and best-positioned actors" clearly is needed, but despite sophisticated high-level tools, repeated experience shows that human error is the principal source of cyber compromise [22], and many serious cybersecurity incidents stem from low-level penetrations, such as those of 2nd of 3rd tier sub-contractors. There still will be a need to make it easier for people to defend themselves more effectively. Zero-Trust Architectures may help, but when will they reach the edges of the networks?

R5. **Recommendation:** *Incentivize research into technical solutions and human engineering practices to make cross-sector security practices simpler and less burdensome for end users during the shift in responsibilities called for by the strategy.*

Shaping the market. Reference [12] calls for "shap[ing] market forces to drive security and resilience." This may be easier said than done in the case of IOT devices. Most economic pressures today focus on functionality and speed to market, not security. The IOT attack surface is exploding and will continue to grow as higher frequency networks with higher device densities proliferate. Research is needed to design such incentives and evaluate how well they work under these conditions. In addition, a more refined regulatory framework may be needed to address failures of the market to incentivize adequate IoT security.

R6. **Recommendation:** *Expand research into design and evaluation of market mechanisms to incentivize security of IoT devices since they inherently cut across sectors.*

R7. **Recommendation:** *Explore further regulatory changes that may be needed to address evolving IoT security needs.*

Coordinating, Synchronizing, and Integrating across sectors. Some of the Sector-Specific plans cite interdependencies, but it is unclear how much preparation and exercising are being done in practice to address these interdependencies.

Most emergency service organizations can protect citizens well within their normal functions and infrastructures, but cascading, cross-sector disruptions require complex public-private collaboration, especially across disaster vs cyber timelines, and public sector vs private sector priorities. One of the best and most integrated studies of the multi-faceted dimensions of these interactions is *A Regional Resilience/Security Analysis Process (RR/SAP) for the Nation's Critical Infrastructure Systems* [23], a quantitative, objective, repeatable business process for "identifying and evaluating ways that metropolitan regions can enhance their security and resilience within available financial and human resources."

Ongoing training and frequent exercises are essential to effective coordination and synchronization. Such training and exercises are in existing guidance, but the scope and pace of change particularly challenge smaller governments and businesses. AI and automation may help, focused on tailoring best practices based on the guidelines to local staffing, human factors, equipment, and conditions (see Recommendation R4 above).

R8. ***Recommendation:*** *Provide incentives and organizational support for training and exercises on cross-sector, cascading disasters. These exercises should involve public and private actors in multiple sectors.*

Specific threat research should analyze the evolving cyber threat landscape during disaster events based on specific locations of interest. As shown in [23] such local coordination is very complex, and hence it is hard to generalize details of approaches. Understanding the tactics, techniques, and procedures used by threat actors can help develop targeted mitigation strategies. The potential consequences of these attacks should focus on the impacts on people not just infrastructure.

Updating sector-specific plans. As noted in [1], the Sector-Specific Plans examined for the Information Technology, Communications, Energy, Transportation, and Emergency Services sectors were dated 7-10 years ago, and many changes have occurred that should be incorporated into new versions. Any guidance needs to increase emphasis on interconnections between sectors and the need for cross-cutting planning and operations. For example, we have been speaking with members of most of the emergency management, public safety (police, fire, EMT) and related organizations in Fairfax County and nearby areas of Northern Virginia. They feel that the Commonwealth of Virginia has an effective set of cross-cutting organizations to keep them up to date on changes to high-level guidance in areas with which they are familiar, but this does not necessarily translate to cross-infrastructure familiarity. For example, a very competent and well-regarded police chief in Northern Virginia completely changed her confident tune when cybersecurity was brought up. Moreover, smaller municipalities with fewer resources need support of guidance tailored to local circumstances.

R9. ***Recommendation:*** *Update SSPs to reflect recent high-level strategic guidance on cross-sector planning and coordination.*

Addressing adaptation. Much work has been done on the “withstand” and “respond” components of resilience, but much less on adaptability. This should be the focus of dedicated research, based on vulnerable scenarios.

R10. ***Recommendation:*** *Develop a comprehensive, wide-ranging, and plausible set of cross-sector disruption/disaster scenarios against which adaptation strategies can be assessed and evaluated. These scenarios should be forward-looking, taking account of anticipated future climate conditions and political situations.*

Given the increasing complexity and growing cross-sector linkages in our nation’s infrastructure, more attention must be paid to adaptation as part of building resilience to cross-sector cascading disruptions.

R11. ***Recommendation:*** *Incentivize research and development to improve the ability to adapt critical infrastructure to be more resilient against the scenarios defined under Recommendation R10, with attention to adequately addressing cross-sector impacts.*

R12. ***Recommendation****: Conduct more research into the coupling functions among power grids, communications nets (especially industrial control systems and emergency comms), and the transport of repair crews.*

Digital twins and simulations offer promise for such study, since closed form models only go so far. Some solutions need not be complex. For example, redundant power at key locations (extra batteries or fuel) could be installed at key network nodes as identified in vulnerability assessments. Cybersecure microgrids linking comms with distributed renewable energy have been demonstrated, for example DoD’s SPIDERS Joint Capability Technology Demonstrator (JCTD) project [24] and their deployment in underserved regions (like Puerto Rico) should be prioritized.

Organizational learning. The growing penetration of cyber-physical systems into all sectors of our infrastructure creates difficult management challenges to organizations responsible for securing the nation’s infrastructure. Such systems encompass both operational technology (OT) and information technology (IT) systems. Operators of OT and IT systems have different cultures; the technology evolves on different timelines; and acquisition involves different budget and procurement cycles. The linkages between OT and IT can create large and poorly understood attack surfaces for cyber threats. The IT community has developed process models like DevSecOps [25] and organizational improvement frameworks like the Cybersecurity Maturity Model (CMMC) [26], which are helping to improve security practices in software development. However, there has thus far been little attention to process models and organizational maturity models that include both IT and OT. A notable step in this direction is the IoT Security Maturity Model, which provides guidance to organizations on the security mechanisms and processes to meet organizational needs and requirements [27]. In addition, the Global Resilience Federation’s Operational Resilience Framework (ORF) [28] states that there are plans to expand the ORF Rules to “address the concerns regarding Operational Technology (OT) Systems, Industrial Control Systems (ICS), and the Internet of Things (IoT).”

R13. ***Recommendation****: Extend maturity models and development processes to address both the IT and OT components of complex cross-sector systems-of-systems. This includes both commissioning the development of enhanced process and maturity models, and, once developed, mandating certification in government contracts.*

R14. ***Recommendation****: Examine the best way to conduct life-cycle training for both IT and OT personnel in all sectors on cross-sector threats and mitigation, with or without formal certification processes.*

Design thinking. Design thinking is a versatile process that emphasizes innovative thinking with a focus on the needs of users. It has five phases: Empathize, Define, Ideate, Prototype, and Test [29]. Of these, "empathize" is the most important since it involves listening to stakeholders to understand and incorporate their needs. This is especially important for addressing the cultural and institutional barriers associated with incorporating both the OT and IT aspects of cross-sector collaboration. Incorporating design thinking into the development of new processes and maturity models promises to help organizations to meet the management challenges associated with cross-sector planning and operations. The Department of Energy's National Cyber-Informed Engineering Strategy [30] is a good example of incorporating design thinking over the entire system lifecycle.

R15. ***Recommendation:*** *Incorporate design thinking into development of new process models, maturity models, and training approaches for cross-sector planning and operations for systems involving both OT and IT elements.*

Threat research. Specific threat research should analyze the evolving cyber threat landscape during disaster events based on specific locations of interest. Understanding the tactics, techniques, and procedures used by threat actors can help develop targeted mitigation strategies. The potential consequences of these attacks should focus on the impacts on people, not just physical infrastructure.

R16. ***Recommendation:*** *Conduct research to understand evolving tactics, techniques, and procedures of cyber threats and to develop targeted mitigation practices. Research should prioritize understanding and mitigating consequences on people as well as physical infrastructure.*

Distribution of resources. The distribution of resources is a recurring problem in disaster situations. For example, FEMA's requirement that disaster relief funds be matched at least in part by recipients and be paid only when work is done has had, and is having, a significant negative impact on disaster reconstruction in many cases. Equally problematic is the requirement that funds be used to restore the pre-disaster condition, not a more effective current capability, e.g., renewable energy and modern communications. Moreover, the length of time it takes to move from planning to execution of reconstruction times, often two years or more, undercuts the objective of rapid reconstruction. Recognizing that at least some of this is based in law, the criteria should be researched as the possible basis for policy change to increase the timeliness and impact of the funds.

R17. **Recommendation**: *Conduct research to understand the effects of bureaucratic and legal impediments to distribution of disaster funds.*

R18. **Recommendation**: *Develop models to streamline distribution of disaster recovery resources without compromising accountability.*

Cyber insurance. The role of cyber insurance in incentivizing cybersecurity investments by critical infrastructure owners and operators needs to be reexamined. Some studies suggest that insurance considerations can cause people in disaster-prone areas to make better decisions after disasters based on realistic insurance pricing, while others suggest that insurance claims are often used to push the insured to purchase products (like cyber defense tools) that benefit the insurer. Research can evaluate how insurance policies can support recovery and adaptation efforts after cyber incidents accompanying disasters.

R19. **Recommendation**: *Conduct research to understand better how insurance policies can be used to incentivize better protection before disasters and improved recovery and adaptation post-disaster.*

Electromagnetic Disturbances. Another vital security need for the future is to protect the energy grid against geomagnetic disturbance (GMD) and/or electromagnetic pulse (EMP). These events can be natural or due to the detonation of a nuclear weapon. They can cause severe disruption and permanent damage to electronic components of our infrastructure and the entire electromagnetic grid, though each involves different damage mechanisms (GMD generally involves long-duration E3 pulses, while EMP involves short-duration E1 ones). The National Coordinating Center for Communications has developed guidelines for EMP protection and resilience [31]. They provide a range of choices from simple, low-cost options for protective measures to more effective and expensive ones. However, the guidance does not call for exercising, and local organizations are more likely to evaluate EMP as a lower priority threat.

R20. **Recommendation**: *Encourage organizations in proximity to critical facilities, or those located in higher risk areas (typically in northern latitudes and closer to the coasts) to exercise counter-EMP procedures.*

Conclusion

High-level guidance on infrastructure resilience and cybersecurity emphasizes the need for cross-sector planning and collaboration, but there remain barriers to turning that guidance into practice. The greatest need in protecting against cascading, multi-sector disruptions is to support organizations and people in tailoring available guidance to local needs and implementing the guidance for their circumstances. The recommendations offered above are directed toward addressing these challenges.

References

[1] L. Wells II and K. B. Laskey, “Policy and Regulations for Enabling Coordinated, Cross-Sector Planning and Operation of Critical Cyber and Physical Infrastructures: Strengths and Limitations,” George Mason University Center for Resilient and Sustainable Communities, Aug. 2023.

[2] OMB, “Circular No. A-130 - Managing Information as a Strategic Resource.” Office of Management and Budget, Jul. 2016. [Online]. Available: https://www.cio.gov/policies-and-priorities/circular-a-130/

[3] FEMA, “National Incident Management System, 3rd Edition,” Oct. 2017. [Online]. Available: https://www.fema.gov/sites/default/files/2020-07/fema_nims_doctrine-2017.pdf

[4] White House, “Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience,” 2013. https://www.cisa.gov/resources-tools/resources/presidential-policy-directive-ppd-21-critical-infrastructure-security-and (accessed Jul. 25, 2023).

[5] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, “Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,” National Institute of Standards and Technology, NIST Special Publication (SP) 800-160 Vol. 2 Rev. 1, Dec. 2021. doi: 10.6028/NIST.SP.800-160v2r1.

[6] C. Zuzak *et al.*, “National Risk Index Technical Documentation,” Federal Emergency Management Agency, Washington, DC, Mar. 2023. [Online]. Available: https://www.fema.gov/sites/default/files/documents/fema_national-risk-index_technical-documentation.pdf

[7] D. Gu, M. Dillard, M. Gerst, and J. Loerzel, “Validating Commonly Used Indicators for Community Resilience Measurement,” *Nat. Hazards Rev.*, vol. 24, no. 2, p. 04023008, May 2023, doi: 10.1061/NHREFO.NHENG-1642.

[8] C. Zuzak, M. Mowrer, E. Goodenough, J. Burns, N. Ranalli, and J. Rozelle, “The national risk index: establishing a nationwide baseline for natural hazard risk in the US,” *Nat. Hazards*, vol. 114, no. 2, pp. 2331–2355, Nov. 2022, doi: 10.1007/s11069-022-05474-w.

[9] CSIAC, “The DoD Cybersecurity Policy Chart – CSIAC,” Jul. 14, 2023. https://csiac.org/resources/the-dod-cybersecurity-policy-chart/ (accessed Jul. 25, 2023).

[10] CISA, “CISA Strategic Plan 2023-2025,” Cybersecurity and Infrastructure Security Agency, Sep. 2022. Accessed: Jul. 31, 2023. [Online]. Available: https://www.cisa.gov/strategic-plan

[11] CISA, “CISA Cybersecurity Strategic Plan FY2024-2026,” Cybersecurity and Infrastructure Security Agency, Aug. 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf

[12] White House, “National Cybersecurity Strategy.” The White House, Oct. 2022. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[13] White House, “National Cybersecurity Strategy Implementation Plan.” The White House, Jul. 2023. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

[14] CISA, “Cross-Sector Cybersecurity Performance Goals, v 1.0.1,” Cybersecurity and Infrastructure Security Agency, Mar. 2023. Accessed: Jul. 25, 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf

[15] CISA, “Energy Sector-Specific Plan,” Cybersecurity and Infrastructure Security Agency, 2015. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf

[16] CISA, “Communications Sector-Specific Plan,” Cybersecurity and Infrastructure Security Agency, 2015. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf

[17] CISA, “Transportation Systems Sector-Specific Plan - 2015,” Cybersecurity and Infrastructure Security Agency, 2015. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf

[18] CISA, “Information Technology Sector-Specific Plan 2016,” Cybersecurity and Infrastructure Security Agency, 2016. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-01/nipp-ssp-information-technology-2016-508%20%281%29.pdf

[19] CISA, “2015 Emergency Services Sector-Specific Plan,” 2015. [Online]. Available: https://www.cisa.gov/resources-tools/resources/emergency-services-sector-specific-plan-2015

[20] “Incident Response Training | CISA,” Sep. 06, 2023. https://www.cisa.gov/resources-tools/programs/Incident-Response-Training (accessed Aug. 29, 2023).

[21] DHS, “The National Cyber Incident Response Plan (NCIRP),” Department of Homeland Security, Dec. 2016. Accessed: Aug. 29, 2023. [Online]. Available: https://www.cisa.gov/resources-tools/resources/national-cyber-incident-response-plan-ncirp

[22] https://www.facebook.com/thehackernews, “Why Human Error is #1 Cyber Security Threat to Businesses in 2021,” *The Hacker News*. https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html (accessed Aug. 02, 2023).

[23] J. P. Brashear *et al.*, “A Regional Resilience/Security Analysis Process For The Nation’s Critical Infrastructure Systems.” ASME Innovative Technologies Institute, 2011. Accessed: Sep. 20, 2022. [Online]. Available: https://www.wbdg.org/files/pdfs/asme_resilience_infrastructure_dec2011.pdf

[24] “Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) Joint Capability Technology Demonstration (JCTD),” Naval Facilities Engineering Command, Technology Transition Final Public Report, Dec. 2015. [Online]. Available: https://www.energy.gov/sites/prod/files/2016/03/f30/spiders_final_report.pdf

[25] H. Myrbakken and R. Colomo-Palacios, “DevSecOps: A Multivocal Literature Review,” in *Software Process Improvement and Capability Determination*, A. Mas, A. Mesquida, R. V. O’Connor, T. Rout, and A. Dorling, Eds., in Communications in Computer and Information Science. Cham: Springer International Publishing, 2017, pp. 17–29. doi: 10.1007/978-3-319-67383-7_2.

[26] W. Gamble, *The Cybersecurity Maturity Model Certification (CMMC) – A pocket guide*. IT Governance Publishing, 2020.

[27] Sandy Carielli, Matt Eble, Frederick Hirsch, Ekaterina Rudina, and Ron Zahav, "IoT Security Maturity Model (SMM): Description and Intended Use," Industrial Internet Consortium, White Paper, May 2020. [Online]. Available: https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1.2.pdf

[28] ORF Task Force, "Operational Resilience Framework Rules v1.0." Business Resilience Council of the Global Resilience Federation, Oct. 2022. [Online]. Available: https://static1.squarespace.com/static/60ccb2c6d4292542967cece7/t/6348277f0660983db5e46e6a/1665673088041/ORF+Rules+V1_0.pdf

[29] R. F. Dam and T. Y. Siang, "5 Stages in the Design Thinking Process," *The Interaction Design Foundation*. https://www.interaction-design.org/literature/article/5-stages-in-the-design-thinking-process (accessed Jan. 10, 2021).

[30] DOE, "National Cyber-Informed Engineering Strategy," US Department of Energy, Jun. 2022. [Online]. Available: https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf

[31] NCC, "Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment." Cybersecurity and Infrastructure Security Agency, Feb. 05, 2019. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/19_0307_CISA_EMP-Protection-Resilience-Guidelines.pdf