Updated to Aug 7, 2023

Policy and Regulations for Enabling Coordinated, Cross-Sector Planning and Operation of Critical Cyber and Physical Infrastructures: Strengths and Limitations[1]

Linton Wells II, Executive Advisory, Center for Resilient and Sustainable Communities (C-RASC), George Mason University

Kathryn Blackmond Laskey, Director Emerita, Center for Resilient and Sustainable Communities, George Mason University

Abstract

As climate change accelerates the frequency of disruptive events, and critical infrastructures become increasingly interdependent, there is a growing need to ensure the policies and standards for the nation's critical infrastructure, including cyber-physical systems, are sufficiently robust and adaptable. This document focuses on elements of five infrastructure sectors that are closely related to DoD planning and operations: energy, communications, transportation, information technology, and emergency services. These have significant interdependencies and crosscutting cybersecurity vulnerabilities, which also are addressed in some detail. It 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-sectoral planning and operation of critical cyber and physical infrastructures. A large amount of very good high-level guidance is available which emphasizes the need for cross-sector collaboration and the incorporation of cybersecurity. But turning these into effective plans and operations is hard. A regional area is used as a case study to illustrate the complex interactions that are needed to align public-private elements at the Federal, state, and local levels. The history and context of how existing policies were conceptualized, as well as their limitations are considered, along with emerging threats, including compound ones (cyberattacks in conjunction with man-made or natural disasters). Holes in capabilities and research topics are identified. A follow-on paper will provide recommendations with corresponding justifications to policy and regulatory decision-makers/institutions for cross-sectoral regulatory standards.

[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.

Executive Summary

Bottom Line: An abundance of policy and regulation is available (see chart in Appendix 1). The challenge is to execute what we have at scale and speed, at all levels, public and private [1].

Applicable Regulatory Standards and Policies. Critical infrastructure protection regulations and policy guidance have been evolving in the U.S. since Presidential Decision Directive 63 [2] in 1998. There is now an extensive body of references on cross-sector planning and operations related to resilience to natural disasters and cyberattacks. The extent of the guidance, and its complexity, is shown by the Department of Defense (DoD) Cybersecurity Policy Chart [3] (Appendix 1), which references over 210 standards and policies. These include National Strategies, White House policy directives and memoranda, as well as standards and policies from many Federal agencies. The Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA) primarily focus on emergency management and disaster response, while Cybersecurity and Infrastructure Security Agency (CISA) guidance applies to securing and protecting the nation's critical infrastructure assets from “all hazards” threats. Details on five of the 16 critical infrastructure sectors most applicable to this study are in Appendix 2. The National Institute of Standards and Technology (NIST) publishes dozens of applicable standards and guidance material. CISA’s Cybersecurity Strategic Plan FY24-26 [1] issued on Aug 4, 2023 ties most of them together.

Interdependence and the Need for Cross-Sector Collaboration. Cross-sector collaboration is central to high-level US guidance, given the deep interconnections between different sectors. At the same time, Presidential Policy Directive 21 (PPD-21) *Critical Infrastructure Protection and Resilience* [4] states: "The private sector is primarily responsible for protecting sector infrastructure and assets. CISA helps the private sector predict, anticipate, and respond to sector outages." This public-private division of labor is critical, and many agencies and organizations are working hard to address it. Changes, both social and technical, are needed in policies, culture, and behavior to adapt to increasingly frequent disruptions to increasingly interconnected systems. Interdependencies must be understood, not just to reduce failures, but more importantly to identify ways to enhance the resilience of an overall system and to incorporate new cross-sector interactions into policy and training.

Cross-Sector Planning and Operations. Executing cross-sector collaboration demands that public and private sector entities share information, resources, and expertise. Its goal is for infrastructure owners and operators, government agencies, emergency responders, and other stakeholders to coordinate their actions effectively to address the complex and interconnected challenges posed by natural and man-made disasters and cyber threats. At the national level, DHS (especially FEMA and CISA) and NIST have published excellent frameworks for incident management and planning. FEMA has developed the National Response Framework (NRF) and the National Incident Management System (NIMS). Individual states have their own planning processes and policies. Most states also have a division of emergency management, as do many counties and cities, to adapt the guidance to local conditions and facilitate adjustments as the high-level guidance changes. Coordination also has improved among the single-sector Information Sharing and Analysis Centers (ISACs) [5] and the cross-sector Information Sharing and Analysis Organizations (ISAOs)[6].

Design thinking is a versatile approach that can be applied to critical infrastructure protection. It has five phases: Empathize, Define, Ideate, Prototype, and Test [7]. Of these, "empathize" is the most important since it involves *listening* to stakeholders to understand and incorporate their needs. Design thinking also can help integrate different systems into DoD acquisition and sustainment processes; improve operations and sustainment in complex environments; sequence actions among the phases of resilience (anticipate, withstand, recover, and adapt); and align technical solutions with people, processes, organizations, and resources.

Limitations and Concerns with Respect to Cyberattacks. There are many policies and regulations for countering cyberattacks, with or without natural disasters. Many are well-written, but more work is needed. Despite the existence of crosscutting guidance, emergency responders often focus on familiar physical infrastructure in crises leaving cybersecurity in separate stovepipes. There have been notable recent efforts to address this issue, but the complexity of cross-sector and multi-stakeholder coordination can lead to gaps both in cybersecurity preparedness and execution. *The* Regional Resilience/Security Analysis Process (RR/SAP) [8] is a case study in how to address some of these difficulties. The volume of sometimes conflicting regulations and guidance also can make it very hard for organizations to be compliant. A common thread in nearly all recent U.S. cyber security breaches is that affected agencies have been trying to follow established risk management standards. But major compromises like the OMB personnel records and SolarWinds challenge us to ask how effective existing approaches are, or even can be. Human factors and budgetary constraints can hinder implementation of even the best guidance and cyber threats are continually evolving, faster than the awareness of most operators and policy makers. Zero Trust architectures [9] may help, but there is no enduring solution. Faster iteration and better execution are key.

Organizational Learning Challenges. Because smart, connected cyber-physical systems involve both operational technology (OT), like generators, and information technology (IT) systems, they pose additional management and security challenges. Operators of OT and IT systems have different cultures, the technology evolves on different timelines, and acquisition involves different budget and procurement cycles. An organization's leadership needs to recognize these challenges and address them. Episodic documentation of "lessons learned" won't work. Continuous learning is needed to create behavior change that evolves at the pace of the systems being considered. Current IT maturity models need to be extended to include OT elements however different they may be. There are some encouraging moves in this direction.

Future Research Needs. This section identifies holes in policies and regulations related to the infrastructures and steps needed to close them, as well as to counter crosscutting cyberattacks during natural and anthropogenic disasters. A key conclusion is that more high-level guidance is needed less than finding ways to help local operators meet the complex demands of the current guidance. Most emergency service organizations can protect citizens well within their normal functions and infrastructures, but cascading, cross-sector disruptions require complex public-private collaboration and on timelines that are very different when cyber threats are added in. Ongoing training and exercises are essential. This is in guidance now, but the scope and pace particularly challenge smaller governments and businesses. How can AI and automation help?

Applicable Regulatory Standards and Policies

U.S. policy toward critical infrastructure protection has evolved from Presidential Decision Directive 63 (PDD/NSC-63) *Critical Infrastructure Protection* in May 1998 [2] through Homeland Security Presidential Directive 7 (HSPD-7) in December 2003 [10], to the present Presidential Policy Directive 21 (PPD-21) *Critical Infrastructure Security and Resilience*, February 2013 [4]. Also published in 2013 was the National Infrastructure Protection Plan (NIPP) [11]. NIST published a *Cybersecurity Framework* in 2014 which was updated in 2018 [12]. This framework is aimed at the operators of critical infrastructure. The establishment of CISA in 2018 under DHS represented a significant strengthening of the previous National Programs and Policy Directorate (NPPD). CISA is responsible for safeguarding the nation's critical infrastructure from various threats, including physical attacks, cyberattacks, and other hazards. The trend since 1998 has been to shift responsibilities for critical infrastructure protection from DoD to DHS, refine and prioritize the sectors (there are now 16), increase emphasis on crosscutting, public-private approaches (see, e.g., the 2011 National Research Council report emphasizing the need for public-private collaboration [13]), raise the importance of risk management, add an emphasis on resilience (vice just security), highlight the need for supply chain protection, and accelerate increases in the focus on cyber security, including for cyber-physical systems. Interestingly, in 2021, Jen Easterly, CISA Director, stated: “One could argue we’re in the business of critical infrastructure, and the most critical infrastructure is our cognitive infrastructure, so building that resilience to misinformation and disinformation, I think, is incredibly important.”(cited in [14]).

Serious cyberattacks have been accelerating as these policies have developed, and these trends have generated increasing attention. The U.S. Congress has included more and more cybersecurity-related provisions in legislation over the past five years. In fact, the fiscal year 2021 National Defense Authorization Act (NDAA) “contained 380% more cyber-related provisions than the FY 2017 NDAA” [15]. Recent detections of attacks such as Colonial Pipeline ransomware (2020) [16], SolarWinds supply chain penetration (2021) [17], JBS meatpacking ransomware (2021) [18], Log4j shell vulnerability (2021) [19], the cyberattacks on Ukraine (ongoing) [20], and the current Chinese attacks [21] reinforce that these are not hypothetical concerns.

The strategy/policy responses are integrated in the 2022 U.S. *National Security Strategy* [22] which mentions infrastructure and resilience 29 times each, cybersecurity 6, and disinformation 3. It was followed by a dedicated *National Cybersecurity Strategy* [23] with an extensive implementation plan in 2023 [24]. The key part of the Strategy 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.”

CISA has defined this as their “North Star.”

On August 4, 2023 CISA issued its *FY2024-2026 Cybersecurity Strategic Plan* [1]. It has 3 goals and 9 objectives, plus metrics.

Goal 1: Address Immediate Threats
Goal 2: Harden the Terrain.
Goal 3: Drive Security at Scale

These are described more in Appendix 2

After the National Security Strategy, its cybersecurity adjuncts, and the CISA Cybersecurity Strategy, two of the most important documents are Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience [4] and the National Security Memorandum (NCM) on Improving Cybersecurity for Critical Infrastructure Control Systems (NCM ICCICS) [25]. Notably, PPD 21 recognizes the interdependency of infrastructure sectors: "U.S. efforts shall address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect this infrastructure's interconnectedness and interdependency" [4]. The directive calls out energy and communications as uniquely critical because of their enabling nature, and the IT sector because of its critical role in cyber resilience. The NCM ICCICS establishes an Industrial Control Systems Cybersecurity Initiative as "voluntary, collaborative effort between the Federal Government and the critical infrastructure community to significantly improve the cybersecurity of these critical systems" [25]. These communications reflect an understanding of the interconnectedness of infrastructure sectors, the need for cross-domain collaborative efforts to improve resilience, and the growing importance of cyber threats to functioning of our nation's critical infrastructure.

Below this over-arching national-level guidance, there is a large body of federal regulations and policies relating to all 16 sectors. However, this paper focuses on regulation and guidance of interest to DoD related to cross-sector planning and operations related to resilience to natural disasters and cyberattacks. Details on the 5 most applicable to this study are in Appendix 2. They are: Energy (a multifaceted web of **electricity**, oil, and natural gas resources—this study focuses on electricity), communications (terrestrial, satellite, and wireless systems with many interdependencies) transportation (aviation, **highway and motor carrier**, maritime transportation system, mass transit and passenger rail, pipeline systems, freight rail, postal and shipping—focus on road transport for infrastructure repair). Information Technology is a separate infrastructure whose mission is to identify and protect against cyber threats and vulnerabilities. Some aspects of Emergency Services also apply notable **emergency management**. However, much of the guidance, e.g., Federal Energy Regulatory Commission regulations regarding transmission and wholesale sale of electricity; Environmental Protection Agency regulations regarding emissions from power plants; Federal Highway Administration standards on vehicle safety; state Public Utility Commission regulations on electricity rates, does not directly relate to the purpose of this paper. Besides federal rules, individual states, and often local authorities, have their own regulations and policies.

This complexity is illustrated by the "DoD Cybersecurity Policy Chart,"[3] (Appendix 1) published by DoD's Cybersecurity and Information Systems Information Analysis Center (CSIAC). It captures and organizes "the tremendous breadth of applicable policies, some of which many cybersecurity professionals may not even be aware of, in a helpful organizational scheme." It is the most comprehensive and cross-referenced source on multi-sector infrastructure resilience uncovered in the study.

The originators of the different policies are color-coded in the table, which contains links that lead to the full text of each of the documents. Over 210 references are listed in five broad categories: Organize, Enable, Anticipate, Prepare, and Authorities. More than 110 also apply to infrastructures beyond DoD, e.g., are not Defense strategy or policy documents, DoD directives, Joint publications, etc. At the same time, many DoD initiatives, such as the Cybersecurity Maturity Model Certification (CMMC) framework [26] affect other departments and agencies, both military and civilian. CMMC, for example, “is designed to provide increased assurance to the Department that a defense industrial base (DIB) contractor can adequately protect sensitive unclassified information.” Since many of those contractors will be involved in other infrastructures, their compliance with DoD rules will affect the other operations also.

The Federal Emergency Management Agency (FEMA), part of DHS, is responsible for coordinating the federal government's response to natural and man-made disasters. FEMA standards typically focus on emergency management, disaster response, and recovery efforts. These standards provide guidance to various stakeholders, including state and local governments, private organizations, and individuals, on how to prepare for, respond to, and recover from emergencies and disasters. FEMA’s National Incident Management System (NIMS) [27] provides a comprehensive framework for managing incidents, including the Incident Command System (ICS) for coordinating response efforts across different agencies and jurisdictions. The National Response Framework (NRF) [28] outlines how the whole community (federal, state, local, tribal, private sector, and non-profit organizations) collaborates to respond to emergencies. FEMA encourages states and communities to develop hazard mitigation plans to identify risks and vulnerabilities and implement measures to reduce the impact of future disasters and provides guidelines to improve the resilience of buildings and infrastructure to withstand natural disasters like hurricanes, earthquakes, and floods.

CISA has developed critical infrastructure standards that apply to the 16 sectors to enhance the security and resilience of critical infrastructure assets and systems. CISA works collaboratively with private sector partners to implement and enforce these standards. CISA publishes standards on risk management for Federal facilities, as well as guidelines for facility security [29]. CISA has recently published Cross-Sector Performance Goals [30], “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.”

In sum, FEMA standards primarily focus on emergency management and disaster response, while CISA standards concentrate on securing and protecting the nation's critical infrastructure assets from various threats. Both sets of standards play critical roles in ensuring U.S. safety, security, and resilience.

The National Institute of Standards and Technology (NIST) publishes standards and guidance related to cybersecurity and critical infrastructure resilience. For example, the Framework for Improving Critical Infrastructure Cybersecurity [31] includes "standards, guidelines, and best practices to manage cybersecurity-related risk." In addition, the special publications (SP) 800 series (computer security) includes extensive guidance for design and operation, e.g. NIST SP 800-53B, Control Baselines for Information Systems and Organizations [32]; NIST SP 800-53 Rev 5, Security and Privacy Controls for Information Systems and Organizations.[33]; SP 800-160 Vol. 1 Rev 1, Engineering Trustworthy Secure Systems [34]; SP 800-160 Vol 2 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach [35]. The DoD Cybersecurity Policy Chart, noted above [3], includes links to a complete list of the SP 800 series [36] (202 records) and the SP 1800 series practice guides [37].

Beyond the planning and execution standards above, it's important to consider resilience and related parameters during the design of systems from power grids to cybersecurity devices. For example, the Department of Energy's ***Cyber-Informed Engineering (CIE) Strategy*** [38] provides a framework that encourages a "security by design" mindset and addresses training and workforce development to promote cybersecurity across the whole lifetime of a system. Although developed for the Energy sector, this strategy is being adopted by DoD and other entities. This is addressed in more detail below under "Design Thinking."

Interdependence and the Need for Cross-Sector Collaboration

As climate and technological change accelerate communities need to develop resilience and response policies to meet increasingly severe disruptions. At the same time, infrastructure systems are becoming more interconnected and interdependent in ways that few understand. To respond effectively to these trends and the ongoing cyberattacks noted above, organizations will need to not just "build back" to a pre-crisis status quo, but rather to adapt to the "new" normal environment and become stronger ("bounce forward better"). These changes cannot focus on technology alone, but rather must involve people, processes, organizations, and resources.

While there is no universally agreed definition of resilience, the term generally refers to a system's capacity to cope with adverse circumstances and then adapt to a post-disruption situation. Resilience is commonly decomposed into capabilities that need to be developed to address different phases of a disruptive event. For example, the US National Institute of Standards and Technology (NIST) defines resilience as the capability to anticipate, withstand, recover from, and adapt to [35] a disruptive event (see also [39] for a similar decomposition). Figure 1 illustrates how the performance of a system evolves during these phases. Policies and practices for resilience should address all these phases and should consider interactions between infrastructure sectors.

The power grid is an important use case for the need to address crosscutting issues across all phases of a disruptive event. Severe weather events are increasing and often have major impacts on the power grid. These impacts can in turn cause disruptions to related telecommunications and transportation networks. Figure 2 illustrates the interdependencies. Power nodes have sensors and communication links which feed Supervisory Control and Data Acquisition (SCADA) systems, which usually are tied to grid control centers. Emergency communications also may be affected by the power disruptions, which can cause repairs to be delayed. Furthermore, threat actors can take advantage of disruptions to cause damage when communities are at their most vulnerable [40].

Power losses can disrupt both the sensors and the communications that feed the SCADA systems. This reduces situational awareness (SA) in the grid's control center, which can disrupt power flows across the network, further degrading not only situational awareness but also the ability to take corrective actions. Lack of SA was a major factor in the 2003 US Northeast blackout [41]. Power disruptions also may affect some emergency communications elements and limit the ability to get situational awareness about transportation routes that may be flooded, damaged, or blocked by fallen trees of power lines, or communicate with responders. This can delay the dispatch of repair crews to restore damaged power lines and communications.

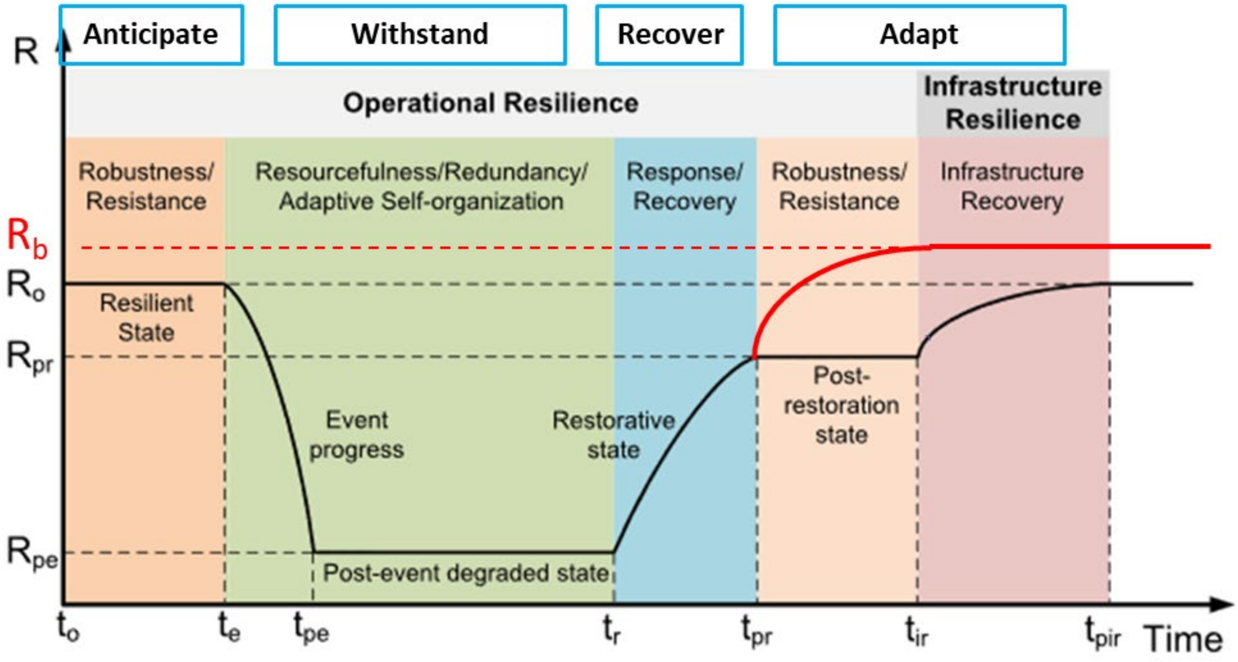


Figure 1: Conceptual resilience curves associated with disruptive events. Horizontal axis denotes time and vertical axis denotes system performance levels. Adapted from [42]

The couplings among the different components are complicated. Numerous studies have looked at various types of interactions, but investigations of "cascading disruptions" often have focused on how a power loss or communications failure can migrate to other sectors, or what steps can be taken to counter it, rather than examining interdependencies, or mutual impacts. The feedback loops between power disruptions and SCADA systems, which can reduce operators' ability to manage power, have not been examined thoroughly [43]. Moreover, the interactions among disrupted transportation, degraded emergency communications and time to repair have rarely been included in analyses.

Nevertheless, there is great potential for improving resilience if interactions among sectors are considered. For example, a simulation-based study [44] showed that accounting for power and communication interdependency in scheduling repairs could increase the total restored energy up to 58% and reduce recovery time up to 63%. Also, ignoring interdependency is likely to cause underestimation of the potential impacts of a disruptive event. Considering interdependencies in an analysis will result in more realistic assessment of potential damage and may enable the damage to be reduced by implementing policies that account for interdependence. This analysis could be extended to distributed energy resources (DER).

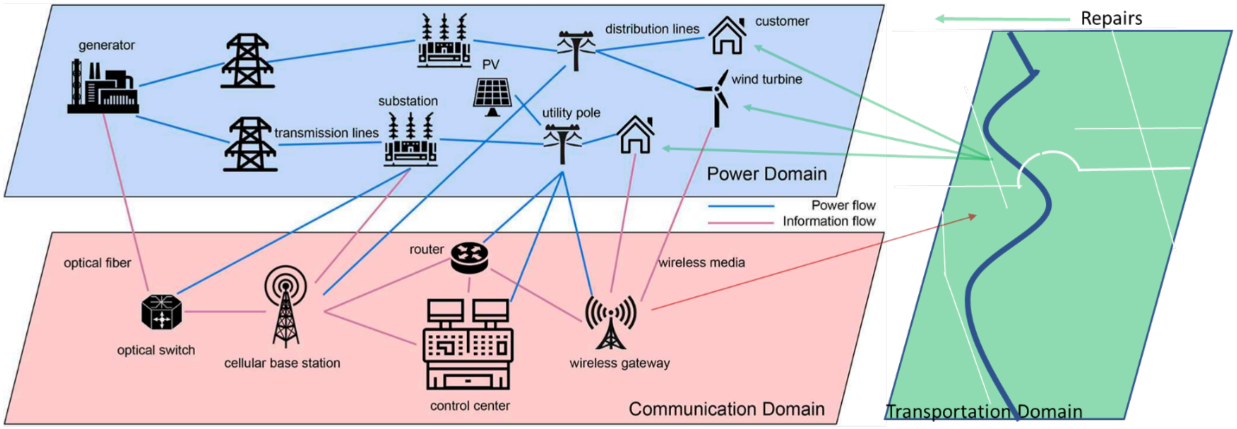


Figure 2: Interdependencies among power, communications and transportation domains.
Adapted from [43]

For several reasons, the importance of incorporating interdependencies among sectors into analyses and policies is growing. First, the projected proliferation of smart grids and smart transportation systems will increase the interdependencies among all these infrastructures. This not only increases the likelihood of coupled disruptions, but also makes it likely that they will happen faster, reducing the options for timely operator intervention [41] [45]   Second, it appears that climate change is increasing the intensity of severe weather events [46], including more extensive flooding, which often makes for more impactful and enduring damage than wind [47]. Finally, increasing amounts of automation makes other infrastructures more reliant on communications and more vulnerable to outages. These links between previously isolated control systems and the Internet significantly expands the cyber “attack surface.” These are not hypothetical threats. As described below, all these types of threats are increasing. The interdependencies must be understood, not just to reduce failures, but more importantly to identify ways to enhance the resilience of the overall system and to incorporate new cross-sector interactions into policy and training.

Cross-Sector Planning and Operations

At both the federal level and in state and local environments, cross-sector collaboration is a critical aspect of planning and operations to counter natural disasters and cyberattacks. PPD-21 is clear that “Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.” But the complex and interconnected challenges posed by natural disasters and cyber threats make it essential that owners and operators be able to benefit from the shared information, expertise and resources of government agencies, emergency responders, and other stakeholders.

Federal, State and Local Guidance and Frameworks for Cross-Sector Planning and Operations

It is important that Federal planners and responders understand not only the full range of guidance down to the local level in an emergency, but also the interests of the local stakeholders since the people most immediately engaged are likely to be from the disaster site itself.

At the national level, DHS (especially FEMA and CISA) and NIST have published excellent frameworks for incident management and planning. The National Infrastructure Protection Plan (NIPP) emphasizes risk management and coordinated efforts among various sectors in protecting critical infrastructure from all hazards. CISA provides guidance, best practices, and support to both federal and state agencies, as well as private sector entities, to enhance their cybersecurity posture. FEMA collaborates with state and local agencies, private sector partners, and non-governmental organizations to address natural disasters and emergencies, ensuring a coordinated and effective response. FEMA’s National Response Framework (NRF) outlines the structure and roles of different partners involved in emergency response and recovery operations to ensure coordination across sectors and levels of government. The National Incident Management System (NIMS) “guides all levels of government, nongovernmental organizations and the private sector to work together to prevent, protect against, mitigate, respond to and recover from incidents” [27].

Regionally, the RRAP [48] seeks to “generate greater understanding and action among public and private sector partners to improve the resilience of a region’s critical infrastructure…. Each RRAP project typically involves a year-long process to collect and analyze data on the critical infrastructure within the designated area, followed by continued technical assistance to enhance the infrastructure’s resilience…. The culmination of RRAP activities, research, and analysis is presented in a Resiliency Assessment report documenting project results and findings, including key regional resilience gaps and options for addressing these shortfalls.” [49] It includes a methodology for assessing regional infrastructure resilience based on 100 projects over 10 years (2009-2019) [50].

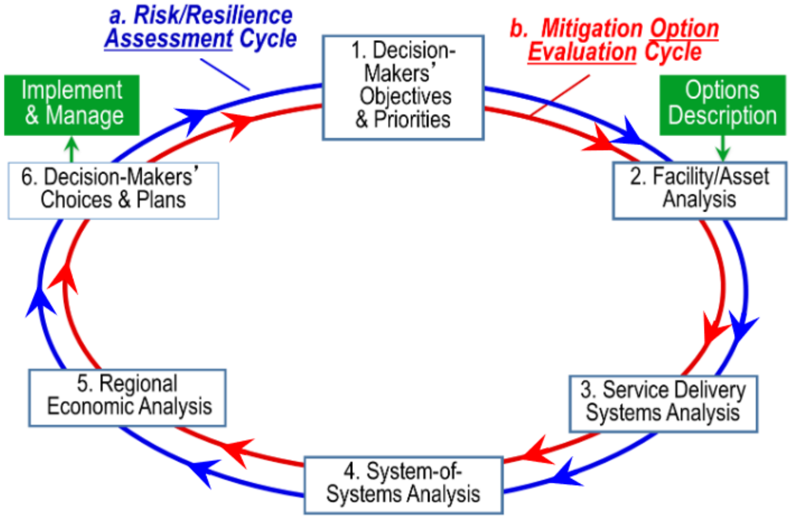
In addition, individual states have their own planning processes and policies. For example, in Virginia, the Virginia Department of Emergency Management (VDEM) "works with local government, state and federal agencies, and voluntary organizations to provide resources and expertise through the four phases of emergency management [prevention and mitigation, preparedness, response, recovery]” [51]. VDEM also develops and maintains state emergency plans and helps communities develop localized plans for emergency operations as well as long-range hazard mitigation. It offers a wide variety of training courses to prepare local first responders, conducts exercises and drills, and aids in crisis response through the Virginia Emergency Operations Center. It also coordinates aid programs with FEMA. The Virginia IT Agency (VITA) and the chief information security officer (CISO) are responsible for IT security and risk management for executive branch agencies.

Below the state level, are county and city structures. For example, the City of Fairfax has an 82-page Emergency Operations Plan [52] which presents a comprehensive framework for managing major emergencies and disaster within the city. It is a "living plan" that can be updated to reflect lessons from exercises or real-world events and is required to be reviewed every four years. It includes plans for alternative communications, critical infrastructure protection, etc., and tasks are aligned with the 15 emergency support functions (ESF) of the NRF.[2]

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* [8]. A diagram of the RR/SAP analysis process is shown below.

The study's design developed from two directions:

> "The first, in order to efficiently advance resilience and security under conditions of uncertainty and severe resource constraints, was to adapt the financial risk analysis and portfolio optimization methods to apply to infrastructure investments on the scale of a metropolitan region. The second, to assure relevance and practicality, was to base RR/SAP on fieldwork in several actual regions with critical infrastructure systems, core community services, and key elements of the business base" [8, p. 2].


a. Risk/Resilience Assessment Cycle
b. Mitigation Option Evaluation Cycle
1. Decision-Makers' Objectives & Priorities
Options Description
2. Facility/Asset Analysis
3. Service Delivery Systems Analysis
4. System-of-Systems Analysis
5. Regional Economic Analysis
6. Decision-Makers' Choices & Plans
Implement & Manage

[2] The Fairfax City Fire Chief, John O'Neil, noted in an interview on July 28, 2023, that the State of Virginia's emergency management structure reviewed changes in higher level guidance and passed them on systematically to cities and counties, greatly relieving the burden on local public safety officials. However, all states may not be well positioned to support local communities. Moreover, even in Virginia, an individual community's ability to execute effective cyber defense is less certain.

Figure 3: The Regional Resilience/Security Analysis Process (RR/SAP) from [8, p. 2]

In considering the decision-makers' objectives and priorities, the study recognized the importance of addressing "All vulnerability, risk, and resilience assessments of their facilities and service delivery systems, from the perspectives of **both** the owners and the community served, respectively" [8, p. 3] (emphasis supplied). In other words, while community interests would naturally focus on areas like resilience and safety, the economic concerns of the infrastructure owners and operators also need to be considered. The 245-page study is a significant contribution to "rational, public-private collaboration toward analysis-based priorities and investments that make regional infrastructure systems and community facilities more resilient, secure and reliable" [8]. This acknowledgement is rare that there are dual public-private objective functions to be satisfied.

In sum, however thorough the high-level guidance is, the effectiveness of the protection of critical infrastructures will depend on how well it's executed locally in times of stress.

Using Design Thinking to Implement Cross-Sector Collaboration

Proposed resilience enhancements need to be implemented in ways that can lead to sustainable capabilities across the life cycles of the systems where they are installed. This is true whether it's a power grid, a communications system, or a cybersecurity device. One approach that has been used successfully in many areas has been "design thinking," which has five phases: Empathize, Define, Ideate, Prototype, and Test [53]. Of these, empathize is the most important since it involves *listening* to stakeholders, whether they are the project managers who might incorporate a capability into their systems, or diverse stakeholders in the community emergency management process, or narrative writers who could advance the case for a particular approach. These are examined in four categories:

- Integrating the different systems into DoD acquisition and sustainment processes
- Operations and Sustainment in Complex Environments
- Sequencing actions among the phases of resilience (anticipate, withstand, recover, and adapt)
- Aligning technical solutions with people, processes, organizations, and resources.

Integrating Different Systems into Federal Acquisition and Sustainment Processes

To get these technical analyses incorporated into the Federal acquisition and sustainment process, proponents will need to understand how they would fit, or could be fit, into a department's processes for design, refit, and operations/sustainment. The DoD acquisition system [54] is used as an example in this paper.

Planning, Design and/or Retrofit Phases

The Department of Energy's *Cyber-Informed Engineering (CIE) Strategy* [38] provides a framework that encourages:

> the adoption of a "security-by-design" mindset within the Energy Sector Industrial Base, which refers to building cybersecurity into our energy systems at the earliest possible stages rather than trying to secure these critical systems after deployment…. CIE further guides our

> cyber workforce development by helping us and our partners focus on the strategic intersection between cybersecurity and engineering, addressing gaps in how we train engineers and technicians and providing them with the means to build in security from the ground up. When our workforce is properly educated and supported, we are better positioned to manufacture and maintain the tools that help us prevent and quickly recover from cyberattacks…. Its recommendations reflect expertise and insight from energy companies, energy systems and cybersecurity manufacturers, standards bodies, researchers, DOE National Laboratories, and Federal partners [emphasis supplied] in the cybersecurity and engineering mission space.

The CIE addresses not only the cybersecurity of the energy infrastructure but also is being adopted by DoD and other entities. For example, one of the offices in the Under Secretary of Defense for Acquisition and Sustainment (USD (A&S))[3] participated in the development of the CIE and is applying it to their workforce development programs for DoD involving diverse cyber-physical systems. A project for the Strategic Environmental R&D Program (SERDP) *Severe Impact Resilience: Assessment Framework for Adaptive Compound Threats* [55] is addressing design features of network control facilities and data centers in the face of compound threats (cyberattacks in conjunction with natural disasters) and has produced two publications [56] [57].

In addition, as noted above, NIST's special publications (SP) 800 series includes extensive guidance for design and operation. This is important and useful guidance, but its complexity may make it challenging for organizations with smaller and/or less mature cybersecurity departments to implement.

A well thought-out and carefully conducted requirements analysis that includes all relevant stakeholders can be thought of as an "empathy" phase in that it identifies those capabilities stakeholders want to have introduced into a system. In DoD, for example, this can be done in several ways, either as an initial requirement through the Joint Requirements Oversight Council (JROC) process, a capability upgrade or retrofit through something like the System Survivability Key Performance Parameter (KPP), a JUON (Joint Urgent Operational Needs Statement) from a Combatant Commander, or as an input from something like the DIU (Defense Innovation Unit). The burden on the developer of a new capability is thus to develop the relationships with the appropriate entry point to get a favorable reading on their proposal. A caution is that it is essential to include all categories of stakeholders and ensure their concerns are fully captured, and the initial capture is the beginning of an enduring, systematic lifecycle-long process.

Operations and Sustainment in Complex Environments

Besides the specific capabilities described above within the power grid, telecommunications network, and transportation domain, different actions need to be taken at different times to build

[3] The *Director, Cyber Warfare, Office of Deputy Assistant Secretary (Platforms and Weapons Portfolio Management), Under Secretary of Defense (Acquisition and Sustainment)* has identified insufficient workforce readiness in cyber resilience of platform systems and the supporting systems they depend on as a priority gap that must be addressed by academia, the commercial and defense industrial base, and the nation."

resilience—the capacity to absorb damage, continue operating through disruption and, critically, to adapt to the post-disruption conditions.

Addressing all Phases of An Adverse Event

Cross-sector planning and operations should consider the phases of an adverse event as depicted in Figure 1 (anticipate, withstand, recover, and adapt). The figure shows how a system's pre-event performance, labeled R_o in the figure, degrades during the event to its post-event value R_{pe}. Then during recovery, performance improves to a post-restoration value R_{pr}. A system that can adapt and "bounce forward" can move to a better performance level R_b.

Anticipate

Building the capability to "anticipate" means taking the time before the disruption to assess existing capabilities, evaluate risk to, and resilience of, both public and private interests, prioritize mitigation measures, and invest accordingly. For example, to prepare against hurricanes, recommended measures are included in [9].

The result will be the performance level indicated by R_o in Figure 1. When multiple infrastructures are involved, subject matter experts from each sector need to be brought together to discuss the links, nodes, and coupling functions between and among them. Location must be considered, with metropolitan areas often receiving the most emphasis because of the impact there, even though rural regions also are at great risk. Design choices also need to consider trade-offs between agility (ability to respond quickly) and robustness (multiple backups). If there are warnings of impending natural disasters, back-up/recovery equipment can be prepositioned in accordance with forecasts. It is critical that these preparations be co-developed with local populations, not only to get buy-in, but also to increase the likelihood that the local responders will be trained and equipped, and that they will continue to improve going forward.

Withstand

To achieve this capability the two most important factors will be (1) the agility/robustness tradeoffs chosen for development during the Anticipate phase, and (2) the ability of the infrastructure operators to identify and respond to threats that could lead to cascading disruptions. The former will largely determine how far R_{pe} is below R_o and how long the post-event disruption lasts. The latter largely will depend on how well situational awareness and ability to execute commands can be maintained for the operators and their ability to identify disruptions due to cyberattacks and respond to them. Within the Withstand and Recover phases these actions occur on very different timelines, as shown in Figure 4 [58]. Some electrical components, like inertia responses and faulty element failures can occur in milliseconds to seconds. Others may extend over days. Cyberattacks also may occur in milliseconds to seconds, so response mechanisms need to be designed to detect and address them, even during simultaneous power grid rebalancing.

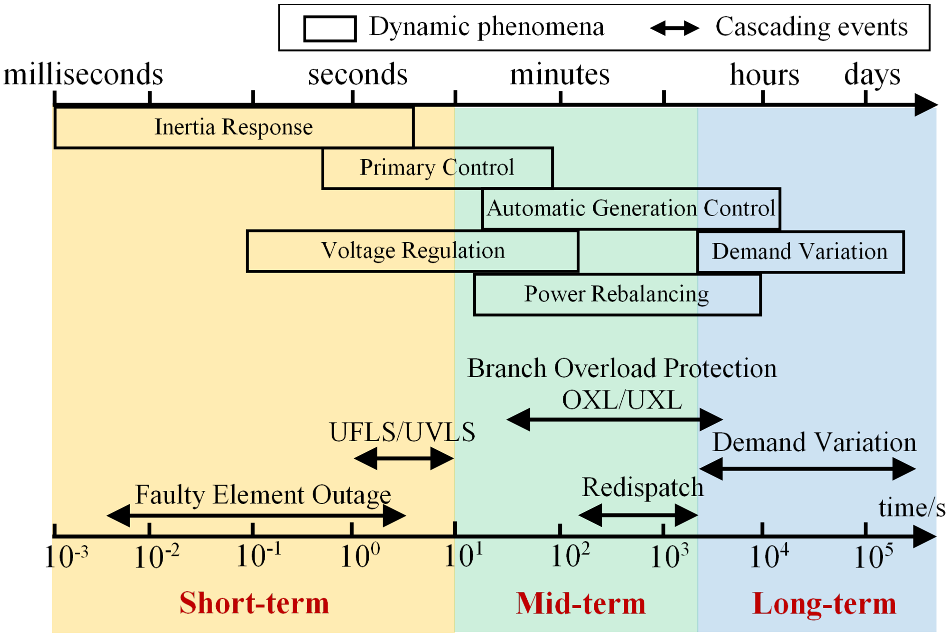


Figure 4: Timescales of typical dynamics involved in cascading failures. Modified in [27] based on [29].

Recover

Continued situational awareness is essential to recovery (or response, robustness/resistance, and infrastructure recovery), not only to understand the state of the grid, but also to vector repair assets to the right place in a timely manner.

Adapt

It is increasingly likely that the post-disruption "new normal" will be different from the pre-disruption situation. Sensing and adapting to these changes will be essential to moving toward a post-disruption state that is an improvement ("bouncing forward better"). Adaptation can include better performance (a higher R_b according to the standard metrics), as well as better ability to withstand and recover from future adverse events. Effective approaches to adaptation deserve additional research lines by themselves. See, for example MITRE's work on "adaptive cyber resiliency for critical operations"[59].

Limitations and Concerns with Respect to Cyberattacks

Between the establishment of CISA to address both cybersecurity and critical infrastructures in a single organization, the National Cybersecurity Strategy and its Implementation Plan, the guidance on operating and protecting critical infrastructures in PPD-21 and related documents, NIST standards, FEMA guidance for emergencies, etc. there would seem to be enough high-level attention and documentation in these areas. Yet successful attacks persist, even without cyberattacks during concurrent disasters.

There is no doubt that the cross-sector attack surface is enormous, and sophisticated attacks from nation-state based Advanced Persistent Threats [60] will continue and sometimes be successful, like the ongoing Chinese penetrations. Sometimes the defenses work, probably more often than we know since successes are rarely publicized [61]. The reasons for the failures are varied, but human error [4] remains the main cause--a major contributing factor in 95% of all breaches according to an IBM estimate. [62] [63]. Other causes include the rise of ransomware (often attributable to human error), supply chain vulnerabilities (as in SolarWinds), and design flaws in key components (e.g., insufficient back-up power).

However, an important question is whether the complexity of the guidance, each part of which may be excellent, exceeds the ability of most operators to follow it.   A common thread in nearly all recent U.S. cyber security breaches is that all the affected agencies have been trying to follow NIST or other established guidance for planning and deploying software systems and then managing them for risk. This is complicated by the fact that there are thousands of sometimes contradictory rules that are poorly coordinated, and any rule that must be interpreted slows the implementation process. The guidance is so complex (see the DoD Cybersecurity Table in Appendix 1) that one wonders if any government office or small/medium-sized business could implement it effectively without extensive outside support, such as from Federally Funded Research and Development Centers (FFRDCs) or specialized contractors. Also, the pace of evolution of both the threat and our own capabilities makes it hard to keep the guidance current. The time factor and the ability to implement are rarely considered in the instructions, nor is the recognition that things inevitably will break. The result is that enormous amounts of time and money are spent trying to interpret, understand, implement, audit, and report out adherence to NIST guidance and associated cyber rules and regulations. Yet continuing major compromises challenge us to ask how effective these approaches are, or even can be.

Also, since infrastructure owners and operators are responsible for the security of their systems, the government's role is mainly advisory. Given commercial and other pressures, many operators will focus on their own infrastructures, vice cross-sector or cybersecurity approaches, despite the overarching guidance. This vulnerability may be exploited by threat actors capitalizing on the chaos of a disaster to launch cyberattacks [40]. There are some notable steps in the right direction. The Industrial Internet Consortium's (IIC) has published and Internet Security Framework, which addresses both the IT and OT aspects of the Industrial Internet of Things [64]. The Global Resilience Federation plans to extend its Operational Resilience Framework to include OT systems, industrial control systems, and the Internet of Things [65]. The IoT Security Maturity Model provides guidance to organizations on the security mechanisms and processes to meet organizational needs and requirements [66].   All these operational approaches need to be underpinned by serious lifecycle engineering.

As noted above, because of the complexity of coordination between emergency management agencies responsible for disaster response and cybersecurity entities, communication and coordination challenges between different agencies and stakeholders could lead to gaps in cybersecurity preparedness. Many states are working hard to reconcile this within their jurisdiction.

[4] In a security context, human error means unintentional actions - or lack of action - by employees and users that cause, spread or allow a security breach to take place [48].

There are laudable efforts to address the challenges of coordination. The RR/SAP, discussed in the previous section, recognizes and was designed to address the complexity and difficulty of coordination not only across sectors but also among public and private stakeholders [8]. A 2011 National Research Council report recognized the need for public-private collaboration to build resilience, and laid out guidelines and strategies for fostering such collaboration [13]. CISA's Regional Resiliency Assessment Program (RRAP) is a voluntary program to allow regions to collect and analyze data on critical infrastructure, assess resilience and knowledge gaps, and improve regional resilience [48]. Coordination also has improved among the single-sector Information Sharing and Analysis Centers (ISACs) through the National Council of ISACs [5], and the cross-sector Information Sharing and Analysis Organizations (ISAOs), through the International Association of Certified ISAOs [6].

In disaster situations, human error can exacerbate cybersecurity vulnerabilities. Responding to cyberattacks during the chaos of a natural disaster can be challenging. The storm or other event evolves more slowly, focusing attention with lots of media coverage and political interest. Staffs working under high-stress conditions may inadvertently fall for phishing attempts or make security mistakes. In these conditions, detection of attacks that take place "machine time" (see Figure 4) may be delayed or missed altogether. Exercises and training in these scenarios are essential, especially since realistic ones inevitably will involve both OT and IT systems.

Budgetary constraints and limited resources may hinder the implementation of robust cybersecurity measures, especially in smaller jurisdictions. Funding allocation might prioritize immediate response and recovery efforts over long-term cybersecurity enhancements, but the "anticipate" and "adapt" phases must be included as well.

Potential solutions include:

- Strengthening coordination between emergency management and cybersecurity entities.
- Increasing awareness and training for disaster response teams about cyber threats.
- Establishing clear lines of communication and information sharing protocols between public and private sector stakeholders.
- Integrating cybersecurity considerations into disaster preparedness and response exercises.
- Encouraging public-private partnerships to pool resources and expertise in cybersecurity efforts.

It is crucial to reassess and update policies and regulations regularly, considering emerging threats and lessons learned from past incidents.

Organizational Learning Challenges

The challenges of integrating the different cultures, systems, paces of technological change and budgets in organizations with cyber-physical systems (which is nearly everyone these days) were noted earlier. Peterson [67] observes that we are asking too much of people in Industrial Control System (ICS) security, noting that consequence reduction often is more effective than likelihood reduction. "Is the control providing the risk reduction you expect? If not, don't do it. Do the right thing correctly and do it well." Herz [68] argues that too much emphasis on innovation can crowd out the redundancy that is necessary for resilience.

Smart, connected cyber-physical systems pose particularly difficult management and security challenges. They involve both operational technology (OT) systems like generators, pumps, and control systems (CS), and information technology (IT) like internet connections. These links can generate very large cyberattack surfaces with poorly understood interdependencies, which are being exploited more and more often. The pace of technological change is very different between OT and IT, e.g., there is little counterpart in the physical world to the agile, near-continuous spirals of DevSecOps [69]. Most importantly, there are large cultural differences between the OT and IT sides of an organization. Safety is an inherent part of the OT environment, but cybersecurity is less so. When a generator fails, the technician is more likely to reach for a multi-meter and a wrench than a cybersecurity patch. From the resource perspective, large OT equipment may be funded through multi-year capital accounts, while IT may be supported by annual operations and maintenance funds. Finally, OT and IT personnel often have come up through different tracks within an organization.

This makes it hard to develop and sustain systems that effectively integrate OT and IT, even though such integration is becoming more common and important, and the consequences of compromise more visible. This puts increased pressure on CPS leadership to respond. Stakeholder engagement on both OT and IT sides is at least as important as any technology to building resilience in the nation's infrastructure. Organizations with CPS will need to learn how to bridge cultural and technological gaps, gain and manage resources from diverse accounts, operate under complex and sometimes conflicting laws and regulations, integrate very different technologies, assure the supply chain from design through end of life, and operate effectively. This will require comprehensive organizational learning approaches.

An important trend is "…the outsourcing of numerous services by OT operators. This includes the integration of IT/OT services…." (CSIAC, 2021) which makes it harder to fold training and team building into the CPS environment.

The divide between OT and IT and the rate of change means that people at all levels need to be trained almost continuously. Since there rarely is time to do this in understaffed and overworked offices, which is one of the causes of the outsourcing of various services by OT operators. In this mix the Cyber Security & Information Systems Information Advisory Center (CSIAC) concludes that "The Integration Service Provider who performs design, installation, configuration, testing, commissioning and handover to the Asset Owner is thought… to be the most important domain expert in the mix of service providers"[70]. In some cases, automation and machine learning could help, but in any case, the integrating service provider will need to be aware of the cross-cultural issues.

Not only must learning be continuous, it must also be accompanied by behavioral change that evolves at the pace of the systems being considered. Such changes often can be informed by reviews conducted by others. The goal of organizational learning is not to reach a final destination--one does not exist. Infrastructure and cybersecurity processes, organizations, and technology, as well as people, are evolving rapidly in ways that often render yesterday's excellent lessons obsolete and create the need for new organizational learning. Innovation births both new problems and opportunities that need to be addressed, especially in the context of saving lives.

Current IT maturity models need to be extended to include OT elements, however different they may be. Simulations have been done and cybersecurity publications written that provide guidance on how organizations can slowly work their way up the maturity ladder [71]. Coupled with testing and simulated threat events, organizations could identify areas where improvements could be made, going beyond the generic implementations recommended by maturity models, and creating lessons that internal staff can individually own and institutionalize, increasing the likelihood of successful execution when needed. There are some encouraging moves in this direction. The Internet Security Framework, developed by the Industrial Internet Consortium (IIC), considers both IT and OT aspects of the Industrial Internet of Things, and "provides guidance as to which mechanisms are to be used and the maturity required to address specific IoT scenarios" [64]. IIC has also developed an IoT security maturity model [66]. This model defines levels of organizational maturity in IoT security: Level 0 (none); Level 1 (minimum); Level 2 (ad hoc); Level 3 (consistent); and Level 4 (formalized). The model provides guidance and metrics for assessing an organization's current level of maturity, evaluating the desired maturity level based on the organization's goals and risks, and defining steps and processes for attaining the desired level. They are similar in concept to the Cybersecurity Maturity Model for IT systems, although a bit different in specifics. The Global Resilience Federation's Operational Resilience Framework [65] 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)."

Future Research Needs

To identify and close holes in policies and regulations related to the infrastructures as well as countering crosscutting cyberattacks during natural and anthropogenic disasters, additional research is needed in various key areas.

One key overarching insight is that local responders and small businesses, especially those in supply chains, need urgent help to meet the complex demands of existing high-level guidance. 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. Ongoing training and frequent exercises are essential. This clearly is in guidance now, 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. Related research should examine the barriers and challenges to information sharing and collaboration between public and private entities before, during, and after disasters. Identifying ways to enhance sharing without compromising sensitive information is crucial.

The Sector-Specific Plans in the areas we examined (Information Technology, Communications, Energy, Transportation, and Emergency Services) all dated from 2014-2016. They doubtless could benefit from research on the many changes that have taken place since the initial issuances. We understand CISA is working on a new strategic framework which can guide the reviews. Any guidance needs to increase emphasis on interconnections between sectors and the need for crosscutting planning and operations.

Within the energy sector, coupling functions among power grids, communications nets (especially industrial control systems and emergency comms), and the transport of repair crews need recurring study. Closed form models so far only go so far, with digital twins and simulations offering promise. The solutions need not be complex. For example, redundant power at key power nodes (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, and their deployment in underserved regions (like Puerto Rico) should be prioritized.

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 infrastructure.

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 Puerto Rican reconstructions after hurricanes Irma and Maria in 2017. There also are requirements that funds be used to build back to the pre-disaster condition, not a more effective current capability, e.g., renewable energy and modern communications. 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.

Much work has been done on the "withstand" and "adapt" components of resilience, but much less on adaptability. This should be the focus of dedicated research, based on vulnerable scenarios.

The role of cyber insurance in incentivizing cybersecurity investments by critical infrastructure owners and operators needs to be examined. 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 other 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 during disasters.

How effective in real world operations are Zero-Trust Architectures likely to be?

By addressing these research needs, policymakers, emergency responders, and cybersecurity professionals can better understand the challenges and opportunities in countering cyberattacks during natural disasters and develop comprehensive strategies to protect critical infrastructure and public safety effectively. Collaboration between academia, government agencies, private sector partners, and non-governmental organizations is essential.

A touchpoint going forward will be to examine closely the goals, objectives and actionable items described in CISA's 2024-2026 Cybersecurity Strategic Plan [1] to understand how to align research with it.

References

[1] "CISA Cybersecurity Strategic Plan FY2024-2026".

[2] The White House, "Critical Infrastructure Protection PDD/NSC-63)." 1998. [Online]. Available: https://irp.fas.org/offdocs/pdd/pdd-63.htm

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

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

[5] "National Council of ISACs," *natlcouncilofisacs*. https://www.nationalisacs.org (accessed Aug. 02, 2023).

[6] "IACI Home - International Association of Certified ISAOs (IACI)." https://www.iaci.global/ (accessed Aug. 02, 2023).

[7] 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).

[8] 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

[9] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[10] The White House, "Homeland Security Presidential Directive 7 |," Dec. 17, 2003. https://www.cisa.gov/news-events/directives/homeland-security-presidential-directive-7 (accessed Jul. 31, 2023).

[11] Department of Homeland Security, "National Infrastructure Protection Plan 2013."

[12] M. P. Barrett, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1." National Institute of Standards and Technology (NIST), Apr. 16, 2018. Accessed: Jul. 25, 2023. [Online]. Available: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

[13] W. Hooke *et al.*, *Building Community Disaster Resilience Through Private-Public Collaboration*. Washington, D.C.: National Academies Press, 2011. doi: 10.17226/13028.

[14] K. K. Fang Lee, "Leaked Documents Outline DHS's Plans to Police Disinformation," *The Intercept*, Oct. 31, 2022. https://theintercept.com/2022/10/31/social-media-disinformation-dhs/ (accessed Jul. 31, 2023).

[15] M. Garcia, "The Militarization of Cyberspace? Cyber-Related Provisions in the National Defense Authorization Act – Third Way," Third Way, Memo, Apr. 2021. Accessed: Jul. 14, 2021. [Online]. Available: https://www.thirdway.org/memo/the-militarization-of-cyberspace-cyber-related-provisions-in-the-national-defense-authorization-act

[16] W. Turton and K. Mehrota, "Hackers Breached Colonial Pipeline Using Compromised Password," *Bloomberg.com*, Jun. 04, 2021. Accessed: Jul. 30, 2023. [Online]. Available:

https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[17] W. Croxton, “Cybersecurity experts say U.S. needs to strike back after SolarWinds hack,” *cbsnews*, Feb. 14, 2021. https://www.cbsnews.com/news/solarwinds-60-minutes-2021-02-14/ (accessed Apr. 03, 2021).

[18] H. Shaban, E. Nakashima, and R. Lerman, “JBS, world’s biggest meat supplier, says its systems are coming back online after cyberattack shut down plants in U.S.,” *Washington Post*, Jun. 01, 2021. Accessed: Jul. 07, 2021. [Online]. Available: https://www.washingtonpost.com/business/2021/06/01/jbs-cyberattack-meat-supply-chain/

[19] J. Reed, “Log4j Forever Changed What (Some) Cyber Pros Think About OSS,” *Security Intelligence*, Jan. 23, 2023. https://securityintelligence.com/articles/log4j-vulnerability-changed-oss-cybersecurity/ (accessed Jul. 30, 2023).

[20] J. A. Lewis, “Cyber War and Ukraine,” CSIS, Jun. 2022. Accessed: Jul. 30, 2023. [Online]. Available: https://www.csis.org/analysis/cyber-war-and-ukraine

[21] D. E. Sanger and J. E. Barnes, “U.S. Hunts Chinese Malware That Could Disrupt American Military Operations,” *The New York Times*, Jul. 29, 2023. Accessed: Aug. 01, 2023. [Online]. Available: https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html

[22] The White House, “Naional Security Strategy 2022.” [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf

[23] 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

[24] White House, “National Cybersecurity Strategy Implementation Plan.” The White House, Jul. 2023.

[25] White House, “National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems,” *The White House*, Jul. 28, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ (accessed Jul. 25, 2023).

[26] OSD, “Cybersecurity Maturity Model Certification (CMMC) Framework - Fact Sheet.” Office of the Secretary of Defense, 2020. [Online]. Available: https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/cmmc/Factsheet-DFARS_Case_2019-D041.pdf

[27] 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

[28] FEMA, “National Response Framework, 4th Edition,” Federal Emergency Management Agency, Oct. 2019. [Online]. Available: https://www.fema.gov/sites/default/files/2020-04/NRF_FINALApproved_2011028.pdf

[29] CISA, “Interagency Security Committee Policies, Standards, Best Practices, Guidance Documents, and White Papers | CISA,” *Cybersecurity and Infrastructure Security Agency*. https://www.cisa.gov/resources-tools/groups/interagency-security-committee-isc/policies-standards-best-practices-guidance-documents-and-white-papers (accessed Jul. 26, 2023).

[30] 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

[31] NIST, "Framework for Cyber-Physical Systems: Volume 1, Overview, Verson 1.0," Special Publication 1500–201, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf

[32] JOINT TASK FORCE, "Control Baselines for Information Systems and Organizations," National Institute of Standards and Technology, Oct. 2020. doi: 10.6028/NIST.SP.800-53B.

[33] Joint Task Force Interagency Working Group, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Sep. 2020. doi: 10.6028/NIST.SP.800-53r5.

[34] R. Ross, M. Winstead, and M. McEvilley, "Engineering trustworthy secure systems," National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST SP 800-160v1r1, Nov. 2022. doi: 10.6028/NIST.SP.800-160v1r1.

[35] 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.

[36] "CSRC List of NIST SP Series Publications." Accessed: Jul. 29, 2023. [Online]. Available: https://csrc.nist.gov/publications/sp800

[37] NIST, "CSRC list of SP 1800 Series practice guides."

[38] US Department of Energy, "National Cyber-Informed Engineering Strategy." DOE, Jun. 2022.

[39] DHS, "National Preparedness Goal - Second Edition," Sep. 2015.

[40] D. Howard, "Hackers Attack When Communities Are Most Vulnerable," *Government Technology*, Sep. 30, 2021. [Online]. Available: https://www.govtech.com/security/hackers-attack-when-communities-are-at-their-most-vulnerable

[41] U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," Apr. 2004.

[42] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Boosting the Power Grid Resilience to Extreme Weather Events Using Defensive Islanding," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2913–2922, Nov. 2016, doi: 10.1109/TSG.2016.2535228.

[43] X. Liu, B. Chen, C. Chen, and D. Jin, "Electric power grid resilience with interdependencies between power and communication networks – a review," *IET Smart Grid*, vol. 3, no. 2, pp. 182–193, 2020, doi: 10.1049/iet-stg.2019.0202.

[44] X. Liu, B. Zhang, B. Chen, A. Aved, and D. Jin, "Towards Optimal and Executable Distribution Grid Restoration Planning With a Fine-Grained Power-Communication Interdependency Model," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 1911–1922, May 2022, doi: 10.1109/TSG.2022.3149973.

[45] M. Panteli, P. A. Crossley, D. S. Kirschen, and D. J. Sobajic, "Assessing the Impact of Insufficient Situation Awareness on Power System Operation," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2967–2977, Aug. 2013, doi: 10.1109/TPWRS.2013.2240705.

[46] B. A. C. Laboratory Ph D. ,. NASA's Jet Propulsion, "A Force of Nature: Hurricanes in a Changing Climate," *Climate Change: Vital Signs of the Planet*. https://climate.nasa.gov/news/3184/a-force-of-nature-hurricanes-in-a-changing-climate (accessed Sep. 21, 2022).

[47] “Hurricanes and Climate Change,” *Center for Climate and Energy Solutions*. https://www.c2es.org/content/hurricanes-and-climate-change/ (accessed Sep. 21, 2022).

[48] CISA, “Regional Resiliency Assessment Program | CISA.” https://www.cisa.gov/resources-tools/programs/regional-resiliency-assessment-program (accessed Jul. 28, 2023).

[49] CISA, “Regional Resiliency Assessment Program (RRAP) Fact Sheet 2023.” [Online]. Available: https://www.cisa.gov/sites/default/files/2023-06/Regional%20Resiliency%20Assessment%20Program%20%28RRAP%29%20Fact%20Sheet%202023.pdf

[50] “Methodology for Assessing Regional Infrastructure Resilience - Lessons Learned from the Regional Resiliency Assessment Program June 2021”.

[51] “Department of Emergency Management | Virginia.gov.” https://www.virginia.gov/agencies/department-of-emergency-management/ (accessed Aug. 01, 2023).

[52] Fairfax OEM, “City of Fairfax Emergency Operations Plan.” May 2021. [Online]. Available: https://ehq-production-us-california.s3.us-west-1.amazonaws.com/8637b331b5975c3ce6e762d00a225efcd8cdbb4c/original/1621430866/e3e6e5ecdcaadfb02db02b92d87a44d0_City_of_Fairfax_Emergency_Operations_Plan.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIA4KKNQAKICO37GBEP%2F20230802%2Fus-west-1%2Fs3%2Faws4_request&X-Amz-Date=20230802T021348Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-Signature=51c543dd78e9f87154f94169a36cadebf75a35b8ec4a2837ca7e1085cdea38a2

[53] “The 5 Stages in the Design Thinking Process,” *The Interaction Design Foundation*, Jul. 06, 2023. https://www.interaction-design.org/literature/article/5-stages-in-the-design-thinking-process (accessed Jul. 02, 2023).

[54] Office of the Under Secretary of Defense for Acquisition and Sustainment, “DoD Directive 5000.01 The Defense Acquisition System.” Sep. 09, 2020. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500001p.pdf

[55] I. Chiu, “Severe Impact Resilience: Assessment Framework for Adaptive Compound Threats,” *SERDP / ESTCP*, Dec. 2019. https://serdp-estcp.org/projects/details/97a0ffaf-6410-4b14-ae66-8ebe961156f3/rc20-1138-project-overview (accessed Aug. 04, 2023).

[56] S. Bommareddy *et al.*, “Data-Centric Analysis of Compound Threats to Critical Infrastructure Control Systems,” in *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, Baltimore, MD, USA: IEEE, Jun. 2022, pp. 72–79. doi: 10.1109/DSN-W54100.2022.00022.

[57] M. Lotfi *et al.*, “A Resilience Assessment Framework for Coupled Power and Communication Infrastructure,” in *Proceedings of the 2023 IEEE Power and Energy Society General Meetings*, Orlando, FL: IEEE, Jul. 2023.

[58] Y. Dai, R. Preece, and M. Panteli, “Benefits and Challenges of Dynamic Modelling of Cascading Failures in Power Systems,” presented at the ACCEPTED FOR PRESENTATION IN 11TH BULK POWER SYSTEMS DYNAMICS AND CONTROL SYMPOSIUM (IREP 2022), 2022, p. 10.

[59] B. Wood, “Adaptive Cyber Resiliency for Critical Operations,” Mar. 2023, Accessed: Aug. 04, 2023. [Online]. Available: https://www.mitre.org/news-insights/impact-story/adaptive-cyber-resiliency-critical-operations

[60] “Advanced Persistent Threats and Nation-State Actors | Cybersecurity and Infrastructure Security Agency CISA.” https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats-and-nation-state-actors (accessed Aug. 02, 2023).

[61] “How do we know when cyber defenses are working?” *Brookings*. https://www.brookings.edu/articles/how-do-we-know-when-cyber-defenses-are-working/ (accessed Aug. 02, 2023).

[62] 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).

[63] M. Ahola, “The Role of Human Error in Successful Cyber Security Breaches.” https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches (accessed Aug. 02, 2023).

[64] IIC, “Industrial Internet Security Framework,” *Industry IoT Consortium*. https://www.iiconsortium.org/iisf/ (accessed Jul. 27, 2023).

[65] ORF Task Force, “Operational Resilience Framework Rules v1.0.” Business Resilience Council of the Global Resilience Federation, Oct. 2022.

[66] 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

[67] “Less ... The Answer To ICS Security,” presented at the ICS CyberSec 2021, Israel, Apr. 28, 2021. Accessed: Jul. 06, 2021. [Online]. Available: https://www.youtube.com/watch?v=7NuLVJLOyW4

[68] J. Herz, “A plea to the Pentagon: Don’t sacrifice resilience on the altar of innovation,” *Atlantic Council*, May 04, 2021. https://www.atlanticcouncil.org/blogs/new-atlanticist/a-plea-to-the-pentagon-dont-sacrifice-resilience-on-the-altar-of-innovation/ (accessed Jul. 05, 2021).

[69] 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.

[70] Cyber Security & Information Systems Information Analysis Center (CSIAC), “Emerging Operational Technology (OT) Cybersecurity Services.” unpublished, May 2021.

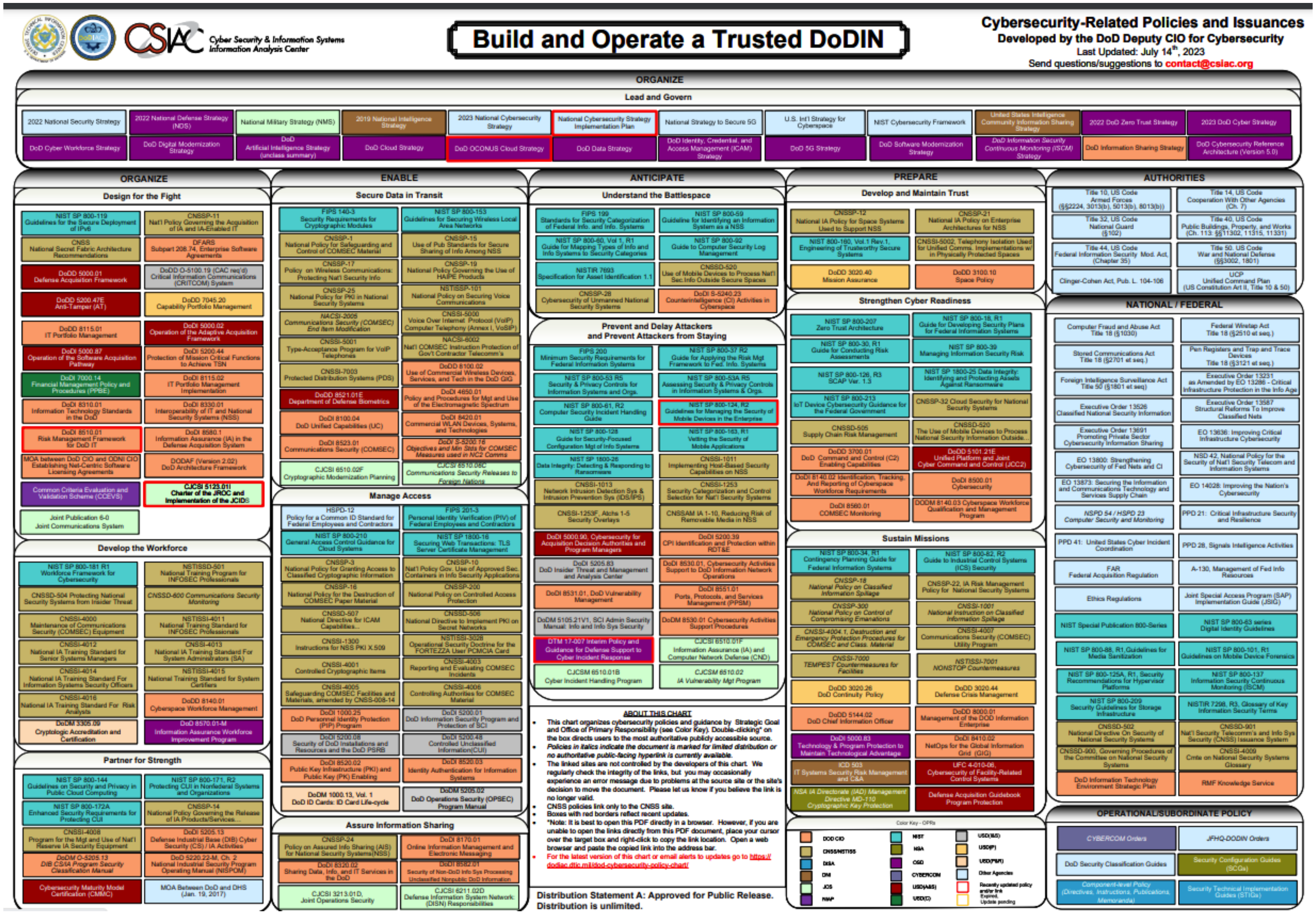
[71] W. Gamble, *The Cybersecurity Maturity Model Certification (CMMC) – A pocket guide*. IT Governance Publishing, 2020.

[72] CISA, “2023-2025 Strategic Plan.” https://www.cisa.gov/strategic-plan (accessed Jul. 31, 2023).

Updated to Aug 7, 2023

Appendix 1

Cybersecurity-Related Policies and Issuances



Cyber Security & Information Systems Information Analysis Center

Build and Operate a Trusted DoDIN

Cybersecurity-Related Policies and Issuances
Developed by the DoD Deputy CIO for Cybersecurity
Last Updated: July 14th, 2023
Send questions/suggestions to contact@csiac.org

ORGANIZE

Lead and Govern

- 2022 National Security Strategy
- 2022 National Defense Strategy (NDS)
- National Military Strategy (NMS)
- 2019 National Intelligence Strategy
- 2023 National Cybersecurity Strategy
- National Cybersecurity Strategy Implementation Plan
- National Strategy to Secure 5G
- U.S. Int'l Strategy for Cyberspace
- NIST Cybersecurity Framework
- United States Intelligence Community Information Sharing Strategy
- 2022 DoD Zero Trust Strategy
- 2023 DoD Cyber Strategy
- DoD Cyber Workforce Strategy
- DoD Digital Modernization Strategy
- DoD Artificial Intelligence Strategy (unclass summary)
- DoD Cloud Strategy
- DoD OCONUS Cloud Strategy
- DoD Data Strategy
- DoD Identity, Credential, and Access Management (ICAM) Strategy
- DoD 5G Strategy
- DoD Software Modernization Strategy
- *DoD Information Security Continuous Monitoring (ISCM) Strategy*
- DoD Information Sharing Strategy
- DoD Cybersecurity Reference Architecture (Version 5.0)

ORGANIZE

Design for the Fight

- NIST SP 800-119 Guidelines for the Secure Deployment of IPv6
- CNSSP-11 Nat'l Policy Governing the Acquisition of IA and IA-Enabled IT
- CNSS National Secret Fabric Architecture Recommendations
- DFARS Subpart 208.74, Enterprise Software Agreements
- DoDD 5000.01 Defense Acquisition Framework
- DoDD O-5100.19 (CAC req'd) Critical Information Communications (CRITCOM) System
- DoDD 5200.47E Anti-Tamper (AT)
- DoDD 7045.20 Capability Portfolio Management
- DoDD 8115.01 IT Portfolio Management
- DoDI 5000.02 Operation of the Adaptive Acquisition Framework
- DoDI 5000.87 Operation of the Software Acquisition Pathway
- DoDI 5200.44 Protection of Mission Critical Functions to Achieve TSN
- DoDI 7000.14 Financial Management Policy and Procedures (PPBE)
- DoDI 8115.02 IT Portfolio Management Implementation
- DoDI 8310.01 Information Technology Standards in the DoD
- DoDI 8330.01 Interoperability of IT and National Security Systems (NSS)
- DoDI 8510.01 Risk Management Framework for DoD IT
- DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System
- MOA between DoD CIO and ODNI CIO Establishing Net-Centric Software Licensing Agreements
- DODAF (Version 2.02) DoD Architecture Framework
- Common Criteria Evaluation and Validation Scheme (CCEVS)
- **CJCSI 5123.01I Charter of the JROC and Implementation of the JCIDS**
- Joint Publication 6-0 Joint Communications System

Develop the Workforce

- NIST SP 800-181 R1 Workforce Framework for Cybersecurity
- NSTISSD-501 National Training Program for INFOSEC Professionals
- CNSSD-504 Protecting National Security Systems from Insider Threat
- *CNSSD-600 Communications Security Monitoring*
- CNSSI-4000 Maintenance of Communications Security (COMSEC) Equipment
- NSTISSI-4011 National Training Standard for INFOSEC Professionals
- CNSSI-4012 National IA Training Standard for Senior Systems Managers
- CNSSI-4013 National IA Training Standard For System Administrators (SA)
- CNSSI-4014 National IA Training Standard For Information Systems Security Officers
- NSTISSI-4015 National Training Standard for System Certifiers
- CNSSI-4016 National IA Training Standard For Risk Analysts
- DoDD 8140.01 Cyberspace Workforce Management
- DoDM 3305.09 Cryptologic Accreditation and Certification
- DoD 8570.01-M Information Assurance Workforce Improvement Program

Partner for Strength

- NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
- NIST SP 800-171, R2 Protecting CUI in Nonfederal Systems and Organizations
- NIST SP 800-172A Enhanced Security Requirements for Protecting CUI
- CNSSP-14 National Policy Governing the Release of IA Products/Services…
- CNSSI-4008 Program for the Mgt and Use of Nat'l Reserve IA Security Equipment
- DoDI 5205.13 Defense Industrial Base (DIB) Cyber Security (CS) / IA Activities
- *DoDM O-5205.13 DIB CS/IA Program Security Classification Manual*
- DoD 5220.22-M, Ch. 2 National Industrial Security Program Operating Manual (NISPOM)
- Cybersecurity Maturity Model Certification (CMMC)
- MOA Between DoD and DHS (Jan. 19, 2017)

ENABLE

Secure Data in Transit

- FIPS 140-3 Security Requirements for Cryptographic Modules
- NIST SP 800-153 Guidelines for Securing Wireless Local Area Networks
- CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material
- CNSSP-15 Use of Pub Standards for Secure Sharing of Info Among NSS
- CNSSP-17 Policy on Wireless Communications: Protecting Nat'l Security Info
- CNSSP-19 National Policy Governing the Use of HAIPE Products
- CNSSP-25 National Policy for PKI in National Security Systems
- NSTISSP-101 National Policy on Securing Voice Communications
- *NACSI-2005 Communications Security (COMSEC) End Item Modification*
- CNSSI-5000 Voice Over Internet Protocol (VoIP) Computer Telephony (Annex I, VoSIP)
- CNSSI-5001 Type-Acceptance Program for VoIP Telephones
- NACSI-6002 Nat'l COMSEC Instruction Protection of Gov't Contractor Telecomm's
- CNSSI-7003 Protected Distribution Systems (PDS)
- DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG
- DoDD 8521.01E Department of Defense Biometrics
- DoDI 4650.01 Policy and Procedures for Mgt and Use of the Electromagnetic Spectrum
- DoDI 8100.04 DoD Unified Capabilities (UC)
- DoDI 8420.01 Commercial WLAN Devices, Systems, and Technologies
- DoDI 8523.01 Communications Security (COMSEC)
- *DoDI S-5200.16 Objectives and Min Stds for COMSEC Measures used in NC2 Comms*
- CJCSI 6510.02F Cryptographic Modernization Planning
- *CJCSI 6510.06C Communications Security Releases to Foreign Nations*

Manage Access

- HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors
- FIPS 201-3 Personal Identity Verification (PIV) of Federal Employees and Contractors
- NIST SP 800-210 General Access Control Guidance for Cloud Systems
- NIST SP 1800-16 Securing Web Transactions: TLS Server Certificate Management
- CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information
- CNSSP-10 Nat'l Policy Gov. Use of Approved Sec. Containers in Info Security Applications
- CNSSP-16 National Policy for the Destruction of COMSEC Paper Material
- CNSSP-200 National Policy on Controlled Access Protection
- CNSSD-507 National Directive for ICAM Capabilities…
- CNSSD-506 National Directive to Implement PKI on Secret Networks
- CNSSI-1300 Instructions for NSS PKI X.509
- NSTISSI-3028 Operational Security Doctrine for the FORTEZZA User PCMCIA Card
- CNSSI-4001 Controlled Cryptographic Items
- CNSSI-4003 Reporting and Evaluating COMSEC Incidents
- CNSSI-4005 Safeguarding COMSEC Facilities and Materials, amended by CNSS-008-14
- CNSSI-4006 Controlling Authorities for COMSEC Material
- DoDI 1000.25 DoD Personnel Identity Protection (PIP) Program
- DoDI 5200.01 DoD Information Security Program and Protection of SCI
- DoDI 5200.08 Security of DoD Installations and Resources and the DoD PSRB
- DoDI 5200.48 Controlled Unclassified Information(CUI)
- DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling
- DoDI 8520.03 Identity Authentication for Information Systems
- DoDM 1000.13, Vol. 1 DoD ID Cards: ID Card Life-cycle
- DoDM 5205.02 DoD Operations Security (OPSEC) Program Manual

Assure Information Sharing

- CNSSP-24 Policy on Assured Info Sharing (AIS) for National Security Systems(NSS)
- DoDI 8170.01 Online Information Management and Electronic Messaging
- DoDI 8320.02 Sharing Data, Info, and IT Services in the DoD
- DoDI 8582.01 Security of Non-DoD Info Sys Processing Unclassified Nonpublic DoD Information
- CJCSI 3213.01D, Joint Operations Security
- CJCSI 6211.02D Defense Information System Network: (DISN) Responsibilities

ANTICIPATE

Understand the Battlespace

- FIPS 199 Standards for Security Categorization of Federal Info. and Info. Systems
- NIST SP 800-59 Guideline for Identifying an Information System as a NSS
- NIST SP 800-60, Vol 1, R1 Guide for Mapping Types of Info and Info Systems to Security Categories
- NIST SP 800-92 Guide to Computer Security Log Management
- NISTIR 7693 Specification for Asset Identification 1.1
- CNSSD-520 Use of Mobile Devices to Process Nat'l Sec.Info Outside Secure Spaces
- CNSSP-28 Cybersecurity of Unmanned National Security Systems
- DoDI S-5240.23 Counterintelligence (CI) Activities in Cyberspace

Prevent and Delay Attackers and Prevent Attackers from Staying

- FIPS 200 Minimum Security Requirements for Federal Information Systems
- NIST SP 800-37 R2 Guide for Applying the Risk Mgt Framework to Fed. Info. Systems
- NIST SP 800-53 R5 Security & Privacy Controls for Information Systems and Orgs.
- NIST SP 800-53A R5 Assessing Security & Privacy Controls in Information Systems & Orgs.
- NIST SP 800-61, R2 Computer Security Incident Handling Guide
- NIST SP 800-124, R2 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-128 Guide for Security-Focused Configuration Mgt of Info Systems
- NIST SP 800-163, R1 Vetting the Security of Mobile Applications
- NIST SP 1800-26 Data Integrity: Detecting & Responding to Ransomware
- CNSSI-1011 Implementing Host-Based Security Capabilities on NSS
- CNSSI-1013 Network Intrusion Detection Sys & Intrusion Prevention Sys (IDS/IPS)
- CNSSI-1253 Security Categorization and Control Selection for Nat'l Security Systems
- CNSSI-1253F, Atchs 1-5 Security Overlays
- CNSSAM IA 1-10, Reducing Risk of Removable Media in NSS
- DoDI 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers
- DoDI 5200.39 CPI Identification and Protection within RDT&E
- DoDI 5205.83 DoD Insider Threat and Management and Analysis Center
- DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations
- DoDI 8531.01, DoD Vulnerability Management
- DoDI 8551.01 Ports, Protocols, and Services Management (PPSM)
- DoDM 5105.21V1, SCI Admin Security Manual: Info and Info Sys Security
- DoDM 8530.01 Cybersecurity Activities Support Procedures
- DTM 17-007 Interim Policy and Guidance for Defense Support to Cyber Incident Response
- CJCSI 6510.01F Information Assurance (IA) and Computer Network Defense (CND)
- CJCSM 6510.01B Cyber Incident Handling Program
- *CJCSM 6510.02 IA Vulnerability Mgt Program*

ABOUT THIS CHART

- This chart organizes cybersecurity policies and guidance by Strategic Goal and Office of Primary Responsibility (see Color Key). Double-clicking* on the box directs users to the most authoritative publicly accessible source.
- *Policies in italics indicate the document is marked for limited distribution or no authoritative public-facing hyperlink is currently available.*
- The linked sites are not controlled by the developers of this chart. We regularly check the integrity of the links, but you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.
- CNSS policies link only to the CNSS site.
- Boxes with red borders reflect recent updates.
- *Note: It is best to open this PDF directly in a browser. However, if you are unable to open the links directly from this PDF document, place your cursor over the target box and right-click to copy the link location. Open a web browser and paste the copied link into the address bar.
- For the latest version of this chart or email alerts to updates go to https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/

Distribution Statement A: Approved for Public Release. Distribution is unlimited.

PREPARE

Develop and Maintain Trust

- CNSSP-12 National IA Policy for Space Systems Used to Support NSS
- CNSSP-21 National IA Policy on Enterprise Architectures for NSS
- NIST 800-160, Vol.1 Rev.1, Engineering of Trustworthy Secure Systems
- CNSSI-5002, Telephony Isolation Used for Unified Comms. Implementations w/ in Physically Protected Spaces
- DoDD 3020.40 Mission Assurance
- DoDD 3100.10 Space Policy

Strengthen Cyber Readiness

- NIST SP 800-207 Zero Trust Architecture
- NIST SP 800-18, R1 Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-30, R1 Guide for Conducting Risk Assessments
- NIST SP 800-39 Managing Information Security Risk
- NIST SP 800-126, R3 SCAP Ver. 1.3
- NIST SP 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware
- NIST SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government
- CNSSP-32 Cloud Security for National Security Systems
- CNSSD-505 Supply Chain Risk Management
- CNSSD-520 The Use of Mobile Devices to Process National Security Information Outside…
- DoDD 3700.01 DoD Command and Control (C2) Enabling Capabilities
- DoDD 5101.21E Unified Platform and Joint Cyber Command and Control (JCC2)
- DoDI 8140.02 Identification, Tracking, And Reporting of Cyberspace Workforce Requirements
- DoDI 8500.01 Cybersecurity
- DoDI 8560.01 COMSEC Monitoring
- DODM 8140.03 Cyberspace Workforce Qualification and Management Program

Sustain Missions

- NIST SP 800-34, R1 Contingency Planning Guide for Federal Information Systems
- NIST SP 800-82, R2 Guide to Industrial Control Systems (ICS) Security
- *CNSSP-18 National Policy on Classified Information Spillage*
- CNSSP-22, IA Risk Management Policy for National Security Systems
- *CNSSP-300 National Policy on Control of Compromising Emanations*
- *CNSSI-1001 National Instruction on Classified Information Spillage*
- *CNSSI-4004.1, Destruction and Emergency Protection Procedures for COMSEC and Class. Material*
- CNSSI-4007 Communications Security (COMSEC) Utility Program
- *CNSSI-7000 TEMPEST Countermeasures for Facilities*
- *NSTISSI-7001 NONSTOP Countermeasures*
- DoDD 3020.26 DoD Continuity Policy
- DoDD 3020.44 Defense Crisis Management
- DoDD 5144.02 DoD Chief Information Officer
- DoDD 8000.01 Management of the DOD Information Enterprise
- DoDI 5000.83 Technology & Program Protection to Maintain Technological Advantage
- DoDI 8410.02 NetOps for the Global Information Grid (GIG)
- ICD 503 IT Systems Security Risk Management and C&A
- UFC 4-010-06, Cybersecurity of Facility-Related Control Systems
- *NSA IA Directorate (IAD) Management Directive MD-110 Cryptographic Key Protection*
- Defense Acquisition Guidebook Program Protection

Color Key - OPRs

🟧	DOD CIO	🟦	NIST	⬜	USD(I&S)
🟨	CNSS/NSTISS	🟩	NSA	🟨	USD(P)
🟦	DISA	🟪	OSD	🟧	USD(P&R)
🟫	DNI	🟪	CYBERCOM	🟦	Other Agencies
🟩	JCS	🟥	USD(A&S)	□	Recently updated policy and/or link
🟪	NMP	🟩	USD(C)	□	Expired, Update pending

AUTHORITIES

- Title 10, US Code Armed Forces (§§2224, 3013(b), 5013(b), 8013(b))
- Title 14, US Code Cooperation With Other Agencies (Ch. 7)
- Title 32, US Code National Guard (§102)
- Title 40, US Code Public Buildings, Property, and Works (Ch. 113: §§11302, 11315, 11331)
- Title 44, US Code Federal Information Security Mod. Act, (Chapter 35)
- Title 50, US Code War and National Defense (§§3002, 1801)
- Clinger-Cohen Act, Pub. L. 104-106
- UCP Unified Command Plan (US Constitution Art II, Title 10 & 50)

NATIONAL / FEDERAL

- Computer Fraud and Abuse Act Title 18 (§1030)
- Federal Wiretap Act Title 18 (§2510 et seq.)
- Stored Communications Act Title 18 (§2701 et seq.)
- Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)
- Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)
- Executive Order 13231 as Amended by EO 13286 - Critical Infrastructure Protection in the Info Age
- Executive Order 13526 Classified National Security Information
- Executive Order 13587 Structural Reforms To Improve Classified Nets
- Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing
- EO 13636: Improving Critical Infrastructure Cybersecurity
- EO 13800: Strengthening Cybersecurity of Fed Nets and CI
- NSD 42, National Policy for the Security of Nat'l Security Telecom and Information Systems
- EO 13873: Securing the Information and Communications Technology and Services Supply Chain
- EO 14028: Improving the Nation's Cybersecurity
- *NSPD 54 / HSPD 23 Computer Security and Monitoring*
- PPD 21: Critical Infrastructure Security and Resilience
- PPD 41: United States Cyber Incident Coordination
- PPD 28, Signals Intelligence Activities
- FAR Federal Acquisition Regulation
- A-130, Management of Fed Info Resources
- Ethics Regulations
- Joint Special Access Program (SAP) Implementation Guide (JSIG)
- NIST Special Publication 800-Series
- NIST SP 800-63 series Digital Identity Guidelines
- NIST SP 800-88, R1,Guidelines for Media Sanitization
- NIST SP 800-101, R1 Guidelines on Mobile Device Forensics
- NIST SP 800-125A, R1, Security Recommendations for Hypervisor Platforms
- NIST SP 800-137 Information Security Continuous Monitoring (ISCM)
- NIST SP 800-209 Security Guidelines for Storage Infrastructure
- NISTIR 7298, R3, Glossary of Key Information Security Terms
- CNSSD-502 National Directive On Security of National Security Systems
- CNSSD-901 Nat'l Security Telecomm's and Info Sys Security (CNSS) Issuance System
- CNSSD-900, Governing Procedures of the Committee on National Security Systems
- CNSSI-4009 Cmte on National Security Systems Glossary
- DoD Information Technology Environment Strategic Plan
- RMF Knowledge Service

OPERATIONAL/SUBORDINATE POLICY

- *CYBERCOM Orders*
- *JFHQ-DODIN Orders*
- DoD Security Classification Guides
- Security Configuration Guides (SCGs)
- *Component-level Policy (Directives, Instructions, Publications, Memoranda)*
- Security Technical Implementation Guides (STIGs)

Appendix 2
Additional Information about Key References

FROM CISA LISTING OF CRITICAL INFRASTRUCTURE SECTORS and DOD CYBERSECURITY POLICY CHART (Appendix 1) https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Information Technology: Sector-Specific Agency: Department of Homeland Security. "The nation's growing dependency on IT makes the Information Technology Sector mission – to identify and protect against cyber threats and vulnerabilities - more complex and important every day." https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/information-technology-sector For the Communications Sector, q.v., the IT Sector provides: "critical control systems and services, physical architecture, and Internet infrastructure, and also relies on communications to deliver and distribute applications and services."

From the **IT Sector-Specific Plan 2016 (An Annex to the National Infrastructure Protection Plan 2013).** **https://www.cisa.gov/sites/default/files/2023-01/nipp-ssp-information-technology-2016-508%20%281%29.pdf**

The IT Sector's vision is to "To achieve a sustained reduction in the impact of incidents on the Sector's critical functions." (p. 9). The ITSSP's intent is "to guide the Sector's voluntary, collaborative efforts to improve security and resilience over the next four years." The sector's six critical functions are:

1. Provide IT products and services
2. Provide incident management capabilities
3. Provide domain name resolution services
4. Provide identity management and associated trust support services
5. Provide Internet-based content, information, and communications services; and
6. Provide Internet routing, access, and connection services.

Figure 2-1 (p. 3) describes these functions in more detail. The emergence of the IoT and the growing importance of cyber-physical systems are mentioned, along with the growth of social networking, but artificial intelligence is not. Other sections of the plan outline IT functions, risks, and mitigations; Critical Infrastructure Partners (public, private, and international); risk assessment and mitigation; R&D opportunities; and metrics. Cybersecurity is emphasized throughout, as are partnerships.

SELECTED LISTINGS FROM DOD CYBERSECURITY POLICY CHART (Appendix 1)—due to complexity, categories and sub-categories from the table are in red.

Category: ORGANIZE

Sub-Category: Lead and Govern

The White House, National Security Strategy, October 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf p. 14 Implementing a Modern Industrial and Innovation Strategy section: "We are securing our critical infrastructure, advancing foundational cybersecurity for critical sectors from pipelines to water, and working with the private sector to improve security defenses in technology products. We are securing our supply chains, including through new forms of public-private collaboration, and using public procurement in critical markets to stimulate demand for innovation." p. 34 Securing Cyberspace section, "We aim to deter cyber attacks from state and non state actors and will respond decisively with all appropriate tools of national power to hostile acts in cyberspace, including those that disrupt or degrade vital national functions or critical infrastructure. We will continue to promote adherence to the UN General Assembly-endorsed framework of responsible state behavior in cyberspace, which recognizes that international law applies online, just as it does offline." [NB infrastructure mentioned 29 times, cybersecurity 6]

U.S. Department of Defense (DoD), 2022. National Defense Strategy. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

Key point: US DoD will defend critical networks.

The White House, National Cybersecurity Strategy 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf Pillar One is to Defend Critical Infrastructure.

p. 2 Next-generation interconnectivity is collapsing the boundary between the digital and physical worlds and exposing some of our most essential systems to disruption. [focus on OT-IT integration]. p. 5 "Government's role is to protect its own systems; to ensure private entities, particularly critical infrastructure, are protecting their systems;"

These forward-leaning efforts have laid the foundation upon which this strategy is built. It was developed alongside the National Security Strategy and National Defense Strategy by a broad interagency team and through a months-long consultation process with the private sector and civil society. It is informed by and implements the values of the DFI, the Freedom Online Coalition, and other long-standing efforts to realize a democratic vision for our digital ecosystem. It carries forward the foundational direction of

- Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," National Security Memorandum (NSM) 5, "Improving Cybersecurity for Critical Infrastructure Control Systems," NSM 8, "Improving the Cybersecurity of National Security, Department of Defense (DoD), and Intelligence Community Systems," and other executive actions.
    - including the Software Bills of Material (SBOM) efforts, NIST's Secure Software Development Framework, and related efforts to improve open-source software security.
- OMB Federal zero trust architecture strategy

It integrates cybersecurity into the once-in-a-generation new investments made by the

- Bipartisan Infrastructure Law,
- the Inflation Reduction Act,
- the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act, and
- EO 14017, "America's Supply Chains."

p. 6 This strategy also builds on the work of prior administrations. It replaces the 2018 National Cyber Strategy but continues momentum on many of its priorities, including the collaborative defense of the digital ecosystem. The Administration remains committed to enhancing the security and resilience of U.S. space systems, including by implementing Space Policy Directive 5, "Cybersecurity Principles for Space Systems." The Administration also continues to implement critical efforts to secure next-generation technologies, including through the

- National Artificial Intelligence Initiative and the National Strategy to Secure 5G, among other existing policies and initiatives. This strategy's goals for securing Federal systems and collaborating with the private sector build on
- EO 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," EO 13691,
- "Promoting Private Sector Cybersecurity Information Sharing," and
- EO 13636, "Improving Critical Infrastructure Cybersecurity," and

fit within the frameworks established by

- Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," and
- Presidential Policy Directive 41, "United States Cyber Incident Coordination."

It carries forward and evolves many of the strategic efforts originally initiated by the 2008 Comprehensive National Cybersecurity Initiative

p. 7 Collaboration to address advanced threats will only be effective if **owners and operators of critical infrastructure have cybersecurity protections in place** to make it harder for adversaries to disrupt them. The Administration has **established new cybersecurity requirements in certain critical sectors. In other sectors, new authorities will be required to set regulations that can drive better cybersecurity practices at scale.** This Administration has conducted **sector-specific engagement with industry to construct consistent, predictable regulatory frameworks for cybersecurity that focus on achieving security outcomes and enabling continuity of operations and functions**, while promoting collaboration and innovation.

Private sector entities have made significant commitments to engage in collaborative defense efforts. **The "Shields Up" campaign** preceding Russia's 2022 brutal and unprovoked war on Ukraine, to proactively increase preparedness and promote effective measures to combat malicious activity, **is an example of public-private collaboration that must be scaled and repeated.** We **must build new and innovative capabilities that allow owners and operators of critical infrastructure, Federal agencies, product vendors and service providers, and other stakeholders to effectively collaborate with each other at speed and scale.** Federal agencies that support critical infrastructure providers must enhance their own capabilities and their ability to collaborate with other Federal entities.

When incidents occur, Federal response efforts must be coordinated and tightly integrated with private sector and State, local, Tribal, and territorial (SLTT) partners. Finally, the Federal Government can better support the defense of critical infrastructure by making its own systems more defensible and resilient. This Administration is committed to improving Federal cybersecurity through **long-term efforts to implement a zero-trust architecture strategy and modernize IT and OT infrastructure. In doing so, Federal cybersecurity can be a model for critical infrastructure across the United States for how to successfully build and operate secure and resilient systems.**

PILLAR ONE: DEFEND CRITICAL INFRASTRUCTURE

Within this pillar are five Strategic Objectives

p. 8 **STRATEGIC OBJECTIVE 1.1**: ESTABLISH CYBERSECURITY REQUIREMENTS TO SUPPORT NATIONAL SECURITY AND PUBLIC SAFETY
p. 10 **STRATEGIC OBJECTIVE 1.2**: SCALE PUBLIC-PRIVATE COLLABORATION
p. 11 **STRATEGIC OBJECTIVE 1.3**: INTEGRATE FEDERAL CYBERSECURITY CENTERS
p. 11 **STRATEGIC OBJECTIVE 1.4:** UPDATE FEDERAL INCIDENT RESPONSE PLANS AND PROCESSES

- Consistent with Presidential Policy Directive 41, "United States Cyber Incident Coordination,"— which defines lead roles for the Department of Justice (DOJ), Department of Homeland Security (DHS), and the Office of the Director of National Intelligence in threat, asset, and intelligence response efforts, respectively—CISA will lead a process to update the subordinate National Cyber Incident Response Plan (NCIRP) to o strengthen processes, procedures, and systems to more fully realize the policy that "a call to one is a call to all."
- When incidents do occur, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) will enhance our awareness and ability to respond effectively.
- p. 12 Following major incidents, we will ensure that the cybersecurity community benefits from lessons learned through the Cyber Safety Review Board (CSRB). Established by EO 14028, "Improving the Nation's Cybersecurity," the CSRB brings together public and private sector cybersecurity leaders to review major cyber incidents, conduct authoritative fact-finding, generate insights that will inform and guide industry remediations, and provide recommendations for improving the nation's cybersecurity posture going forward. The Administration will work with Congress to pass legislation to codify the CSRB within DHS and provide it the authorities it needs to carry out comprehensive reviews of significant incidents.

p, 12 **STRATEGIC OBJECTIVE 1.5:** MODERNIZE FEDERAL DEFENSES

The Cybersecurity Strategy overall includes Five Pillars and Under these are 27 Strategic Objectives. The Implementation plan (next below) adds several initiatives, such as "Establish an initiative on cyber regulatory harmonization."

The White House, National Cybersecurity Strategy Implementation Plan, July 2023. <https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf>

National Telecommunications and Information Administration (NTIA), National Strategy to Secure 5G Implementation Plan, January 2021. https://ntia.gov/other-publication/national-strategy-secure-5g-implementation-plan

US National Institute of Standards and Technology (NIST), Cybersecurity Framework, Discussion Draft NIST Cybersecurity Framework 2.0 posted for comment April 2023. Function and Category Names and Identifiers: 6 Functions (Govern, Identify, Protect, Detect, Respond, Recover), 21 categories, 112 subcategories. [NB: this adds Govern] https://www.nist.gov/system/files/documents/2023/04/24/NIST%20Cybersecurity%20Framework%202.0%20Core%20Discussion%20Draft%204-2023%20final.pdf Standards will be posted in NIST's **Cybersecurity and Privacy Reference Tool (CPRT)** https://csrc.nist.gov/projects/cprt

US Department of Defense, DoD Zero Trust Strategy, October 21, 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf p. ii DoD requires an enhanced cybersecurity framework built upon Zero Trust principles that must be adopted across the Department, enterprise-wide, as quickly as possible as described within this document...This “never trust, always verify” mindset requires us to take responsibility for the security of our devices, applications, assets, and services; users are granted access to only the data they need and when needed. 4 goals: ZT culture adoption, DoD Info Systems secured and defended, tech acceleration, ZT enablement.

White House, "Executive Order on Improving the Nation’s Cybersecurity" EO14028. "Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."

NIST, Special Publication 1271, Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide, 6 August 2021. Includes descriptions of cybersecurity core functions and a set of guidelines for mitigating organizational cybersecurity risks.

NIST, SP 800-207, Zero Trust Architecture, August 2020. p. ii. has basic definitions. **NIST 1800-35** **Implementing a Zero Trust Architecture** is open for comment to close 9/4/23. It is a draft practice guide. https://csrc.nist.gov/pubs/sp/1800/35/2prd This guide summarizes how the National Cybersecurity Center of Excellence (NCCoE) and its collaborators are using **commercially available technology to build interoperable, open standards-based ZTA example implementations** that align to the concepts and principles in NIST Special Publication (SP) 800-207, *Zero Trust Architecture*. The updated versions of volumes B and C **describe ten ZTA implementations, demonstrating how blends of commercially available technologies can be integrated and brought into play to build various types of ZTAs.**

OMB, Federal Zero Trust Architecture Strategy "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," OMB Memorandum M-22-09 (26 Jan 2022).

National Security Memorandum-8, Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems (19 January 2022).

There also are various directives on national security systems, and Risk Management Frameworks

Sub-Category: Develop the Workforce

NIST, "Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181 Revision 1, November 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf **National Initiative for Cybersecurity Education (NICE)**. "The NICE Framework has been developed to help provide a reference taxonomy—that is, a common language—of the cybersecurity work and of the individuals who carry out that work. The NICE Framework supports the NICE mission to energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development. The NICE Framework provides a set of building blocks for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams. Key elements = Agility, Flexibility, Interoperability, and Modularity Tasks, Knowledge, and Skills

Subcategory: Partner for Strength

NIST, "Guidelines on Security and Privacy in Public Cloud Computing" NIST SP 800-144, Dec 2011. https://csrc.nist.gov/pubs/sp/800/144/final This publication provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment.

NIST, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," NIST SP 800-171 Rev. 2, Updated to January 2021. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf Published in February 2021, **NIST SP 800-172** is a supplement publication to NIST SP 800-171. It was designed to strengthen supply chain resilience against sophisticated cybersecurity attacks. NIST 800-172 accordingly contains a series of 35 enhanced security controls to safeguard high-risk unclassified information on non-federal systems.... **Advanced Persistent Threat (APT)** is defined in the NIST SP 800-172 publication as an adversary that has the resources and expertise to attack systems through different attack vectors.

Cybersecurity Maturity Model Certification (CMMC) Framework (DFARS Case 2019-D041). https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/cmmc/Factsheet-DFARS_Case_2019-D041.pdf The US government is using CMMC certification as a vehicle to audit compliance with NIST SP 800-171, a publication that recommends requirements for protecting CUI.... CMMC is a certification framework that is designed to ensure contractors' compliance with existing NIST standards, such as NIST SP 800-171 and a subset of NIST SP 800-172. CMMC was created to address the low levels of adoption of NIST SP 800-171 among DoD contractors.... [it may be applicable to up to 200,000). .... The CMMC 2.0 requirements were expected to be in all new contracts by October 2025, but due to the rule-making process, it now seems they won't appear in solicitations until **May 2023**...The three new levels in CMMC 2.0 directly correlate to existing federal requirements: Level 1 (Foundational), Level 2 (Advanced), and Level 3 (Expert)....Level 1 contractors can now perform annual self-assessments, while Level 2 contractors can complete self-assessments and submit senior official affirmations for non-prioritized acquisitions or require third-party assessments for prioritized acquisitions. Level 3 contractors must undergo triennial CMMC certification conducted by government officials.... On average, it takes about 12-18 months for a company with 50-100 employees to get in compliance with the NIST SP 800-171 guidelines, which are the basis for CMMC Level 2. ... The enforcement of CMMC compliance shows how the government can advocate for enhanced cybersecurity protocols without explicitly legislating them. This illustrates the government's ability to use a single approach to compel a greater number of private sector organizations to bolster their security by adopting the CMMC standard. Although it is somewhat based on NIST, the CMMC is an independent certification system not created by the federal government. Nevertheless, it has become mandatory for Department of Defense contractors and subcontractors.

Category: ENABLE

Sub-category: Secure Data in Transit (13 references outside DoD)

NIST, "**Guidelines for Securing Wireless Local Area Networks (WLANs), NIST SP 800-153, February 2012.** The NIST SP 800-153 document was developed to provide security guidance for WLAN connections based on the IEEE 802.11 specification. This standard is meant to supplement, not override any other NIST documents, guidelines, and standards related to communication security. The SP 800-153 is considered one of the vital digital security documents aimed at providing the groundwork for a significant portion of IoT connections, including applications that relate to the smart city/automotive combination.

Manage Access (16 references outside DoD)

The White House, "Policy for a Common Identification Standard for Federal Employees and Contractors," Homeland Security Presidential Directive-12, August 2004. https://www.dhs.gov/homeland-security-presidential-directive-12 Establishes **"**a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)

Category: ANTICIPATE

Sub-Category: Understand the Battlespace (7 references outside DoD)

NIST, Guide for Mapping Types of Information and Information Systems to Security Categories, NIST SP 800-60 Vol 1, August 2008. "...this guideline has been developed to assist Federal government agencies to categorize information and information systems. The guideline's objective is to facilitate application of appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or use of the information or information system."

Sub-Category: Prevent and Delay Attackers and Prevent Attackers from Staying

NIST, Guidelines for Managing the Security of Mobile Devices in the Enterprise, SP 800-124r2, May 2023. Mobile devices were initially personal consumer communication devices, but they are now permanent fixtures in enterprises and are used to access modern networks and systems to process sensitive data. This publication assists organizations in managing and securing these devices by describing available technologies and strategies. Security concerns inherent to the usage of mobile devices are explored alongside mitigations and countermeasures. Recommendations are provided for the deployment, use, and disposal of devices throughout the mobile-device life cycle. The scope of this publication includes mobile devices, centralized device management, and endpoint protection technologies, as well as both organization-provided and personally owned deployment scenarios.

Category: PREPARE

Sub-Category: Develop and Maintain Trust (4 references outside DoD, but on in DoD is very important

Department of Defense, MISSION ASSURANCE (MA), DOD DIRECTIVE 3020.40, updated to Change 1, Sept 11, 2018. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf 1.2 "DoD uses MA as a process to protect or ensure the continued function and resilience of capabilities and assets by refining, integrating, and synchronizing the aspects of the DoD security, protection, and risk-management programs that directly relate to mission execution."

U.S. Department of Defense (DoD), DoD Mission Assurance Strategy, April 2012. https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf"...**defines mission assurance** as: A process to protect or ensure the continued function and resilience of capabilities and assets – including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains – critical to the performance of DoD MEFs in any operating environment or condition.1 Mission assurance focuses on the protection, continued function, and resilience of capabilities and assets critical to supporting MEFs, rather than the operational execution of DoD missions themselves.

Category: AUTHORITIES

Sub-Category: National Federal Guidance (16 standards outside DOD)

The White House, Critical Infrastructure Security and Resilience, PPD-21, February 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil ...**Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.**

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require **integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.**

This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (herein referred to as "critical infrastructure owners and operators"). This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration. The Federal Government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.

PPD-21 assigns Sector-Specific Agencies (SSAs) to each of the 16 sectors (DoD's only sector is the Defense Industrial Base)

> **Communications: Sector-Specific Agency: Department of Homeland Security.** "The private sector is primarily responsible for protecting sector infrastructure and assets. CISA helps the private sector predict, anticipate, and respond to sector outages." https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/communications-sector (More detail is below in The Communications Sector area)
>
> **Energy: Sector-Specific Agency: Department of Energy.** "The energy sector protects a multifaceted web of electricity, oil, and natural gas resources and assets to maintain steady energy supplies and ensure the overall health and wellness of the nation."
> "The Energy Sector is well aware of its vulnerabilities and is leading a significant voluntary effort to increase its planning and preparedness. Cooperation through industry groups has resulted in substantial information sharing of best practices across the sector. Many sector owners and operators have extensive experience abroad with infrastructure protection and have more recently focused their attention on cybersecurity." **https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/** (More detail is below in the Energy Sector area)
>
> **Information Technology: Sector-Specific Agency: Department of Homeland Security.** "The nation's growing dependency on IT makes the Information Technology Sector mission – to identify and protect against cyber threats and vulnerabilities – more complex and important every day." https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/information-technology-sector For the Communications Sector, q.v., the IT Sector provides: "critical control systems and services, physical architecture, and Internet infrastructure, and also relies on communications to deliver and distribute applications and services." (More detail is below in the IT Sector area)

Emergency Services: **Sector-Specific Agency: Department of Homeland Security.** “Supporting millions of skilled personnel with physical and cyber resources, the Emergency Services Sector helps save lives, protect property and the environment, and assist in recovery efforts.” **https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/emergency-services-sector**

Five distinct disciplines compose the ESS, encompassing a wide range of emergency response functions and roles:

- Law Enforcement
- Fire and Rescue Services
- Emergency Medical Services
- **Emergency Management**
- Public Works

The ESS also provides 11 different kinds of specialized emergency services through individual personnel and teams. (More detail is below in the Emergency Services Sector area)

Transportation Sector Systems: **Co-Sector-Specific Agencies: Department of Homeland Security and Department of Transportation** “Moving millions of people and goods across the country every day, CISA protects the transportation systems sector from a limitless number of threats and risks to ensure a continuity of operations.” https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector

The Transportation Systems Sector consists of seven key subsectors, or modes:

- Aviation
- **Highway and Motor Carrier**
- Maritime Transportation System
- Mass Transit and Passenger Rail
- Pipeline Systems
- Freight Rail
- Postal and Shipping

For the purpose of addressing cross-sector, cascading infrastructure disruptions, the principal interactions will most affect highways in that the restoration of most damaged comms and power capabilities will require road access by repair crews. (More detail is below in the Transportation Sector area)

PPD-21 definitions:

- The term “all hazards” means a threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.
- “critical infrastructure” has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to

the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

- “resilience” means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

CISA, 2024-2026 Strategic Plan
CISA Cybersecurity Strategic Plan FY2024-2026
“Our nation is at a moment of opportunity. The 2023 U.S. National Cybersecurity Strategy outlines a new vision for cybersecurity, a vision grounded in collaboration, in innovation, and in accountability. Now is the moment where our country has a choice: to invest in a future where collaboration is a default rather than an exception; where innovation in defense and resilience dramatically outpaces that of those seeking to do us harm; and where the burden of cybersecurity is allocated toward those who are most able to bear it…. We must change how we design and develop technology products, such that exploitable conditions are uncommon and secure controls are enabled before products reach the market. We must quickly detect adversaries, incidents, and vulnerabilities, and enable timely mitigation before harm occurs. We must help organizations, particularly those that are “target rich, resource poor,” take the fewest possible steps to drive the most security impact. Recognizing that we will not prevent every intrusion, we must ensure that our most essential services are resilient under all conditions, with particular focus on under-resourced communities where loss of key services can have the greatest impact. Most importantly, we must do it together, recognizing that true collaboration is the only path toward a more secure future.”

Cybersecurity Strategic Plan outlines three enduring goals: (p. 2)

GOAL 1: ADDRESS IMMEDIATE THREATS. We will make it increasingly difficult for our adversaries to achieve their goals by targeting American and allied networks. We will work with partners to gain visibility into the breadth of intrusions targeting our country, enable the disruption of threat actor campaigns, ensure that adversaries are rapidly evicted when intrusions occur, and accelerate mitigation of exploitable conditions that adversaries recurringly exploit.

GOAL 2: HARDEN THE TERRAIN. We will catalyze, support, and measure adoption of strong practices for security and resilience that measurably reduce the likelihood of damaging intrusions. We will provide actionable and usable guidance and direction that helps organizations prioritize the most effective security investments first and leverage scalable assessments to evaluate progress by organizations, critical infrastructure sectors, and the nation.

GOAL 3: DRIVE SECURITY AT SCALE. We will drive prioritization of cybersecurity as a fundamental safety issue and ask more of technology providers to build security into products throughout their lifecycle, ship products with secure defaults, and foster radical transparency into their security practices so that customers clearly understand the risks they are accepting by using each product. Even as we confront the challenge of unsafe technology products, we must ensure that the future is more secure than the present — including by looking ahead to

> reduce the risks and fully leverage the benefits posed by artificial intelligence and the advance of quantum-relevant computing. Recognizing that a secure future is dependent first on our people, we will do our part to build a national cybersecurity workforce that can address the threats of tomorrow and reflects the diversity of our country.

As we progress toward these goals, **we must embody the hacker spirit, thinking creatively and innovating in every aspect of our work.**

CISA, 2023-25 Strategic Plan. **"**Our nation is at a moment of opportunity. The 2023 U.S. National Cybersecurity Strategy outlines a new vision for cybersecurity, a vision grounded in collaboration, in innovation, and in accountability. Now is the moment where our country has a choice: to invest in a future where collaboration is a default rather than an exception; where innovation in defense and resilience dramatically outpaces that of those seeking to do us harm; and where the burden of cybersecurity is allocated toward those who are most able to bear it. We must be clear-eyed about the future we seek, one in which damaging cyber intrusions are a shocking anomaly, in which organizations are secure and resilient, in which technology products are safe and secure by design and default. This is a shared journey and a shared challenge, and CISA, as America's cyber defense agency, is privileged to serve a foundational role in the global cybersecurity community as we achieve measurable progress to our shared end state."
https://www.cisa.gov/strategic-plan
The Plan focuses on how to "collectively **reduce risk and build resilience to cyber and physical threats to the nation's infrastructure**." It notes that:

> Infrastructures that underpin our National Critical Functions (NCF) cross multiple sectors and continue to grow more interdependent. *NCF are functions of government and the private sector so vital to the U.S. that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof* (emphasis supplied). The boundaries between the nation's cyber and physical infrastructure are therefore increasingly blurred. The convergence of cyber-physical technologies and systems that deliver our critical functions — from manufacturing to healthcare to transportation and beyond — means that single events can manifest in the loss or degradation of service across multiple industries. Operational technology (OT) and industrial control systems (ICS) pose unique risks that demand particular focus due to the heightened consequences of disruption and challenges related to deploying certain security controls at scale.

National Critical Functions (from CISA Strategic Plan [72]**)**

- NCF are functions of government and the private sector so vital to the U.S. that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Department of Homeland Security, National Infrastructure Protection Plan: Partnering for Critical Infrastructure and Resilience, 2013. https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf
The community involved in managing risks to critical infrastructure is wide-ranging, composed of partnerships among owners and operators; Federal, State, local, tribal, and territorial governments; regional entities; non-profit organizations; and academia. Managing the risks from significant threat and hazards to physical and cyber critical infrastructure requires an integrated approach across this diverse community to:

- Identify, deter, detect, disrupt, and prepare for threats and hazards to the Nation's critical infrastructure
- Reduce vulnerabilities of critical assets, systems, and networks; and
- Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.

The success of this integrated approach depends on leveraging the full spectrum of capabilities, expertise, and experience across the critical infrastructure community and associated stakeholders. This requires efficient sharing of actionable and relevant information among partners to build situational awareness and enable effective risk-informed decision making.

This plan "organizes critical infrastructure into 16 sectors and designates a federal department or agency as the lead coordinator—Sector-Specific Agency (SSA)—for each sector…." (See more detail above under PPD-21, and below, under each of the infrastructures relevant to this study).
………………………

The White House, United States Cyber Incident Coordination PPD-41, May 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident Five principles.

1. Shared Responsibility.
2. Risk-Based Response.
3. Respecting affected entities.
4. Unity of Governmental Effort.
5. Enabling Restoration and Recovery.

The **Cyber Response Group (CRG)**, in support of the National Security Council (NSC) Deputies and Principals Committees, and accountable through the Assistant to the President for Homeland Security and Counterterrorism (APHSCT) to the NSC chaired by the President, shall **coordinate the development and implementation of** United States Government **policy and strategy** with respect to significant cyber incidents affecting the United States or its interests abroad.
Cyber Unified Coordination Group. A **Cyber Unified Coordination Group (UCG)** shall serve as the primary method for coordinating between and among Federal agencies in response to a significant cyber incident as well as for integrating private sector partners into incident response efforts, as appropriate.

NIST, Computer Security Resource Center SP 800 series guidance documents https://csrc.nist.gov/publications/sp800 202 matching records

NIST, Computer Security Resource Center SP 1800 series practice guides
https://csrc.nist.gov/publications/sp1800 34 matching records

Sub-Category: Operational/Subordinate Policy (all DOD)

Of the above, three are recently changed:

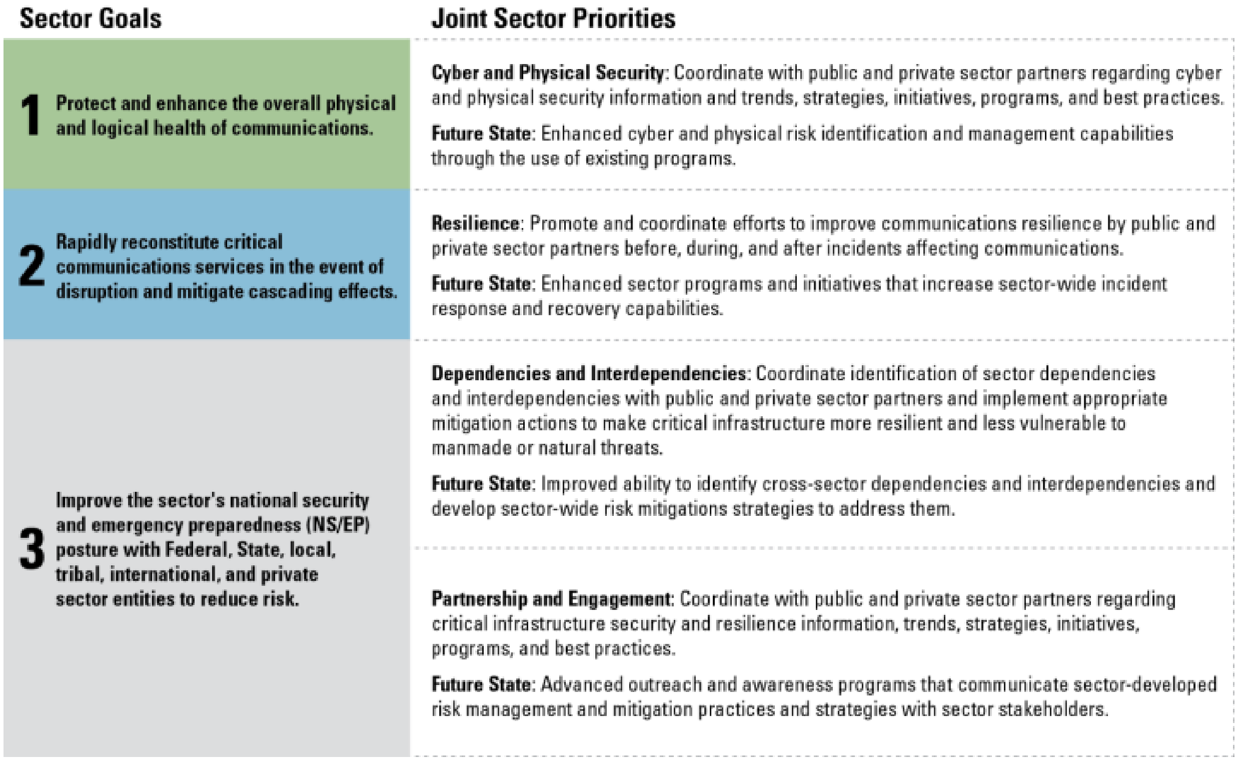
- **National Cybersecurity Strategy Implementation Plan July 2023**
- Guidelines for Managing the Security of Mobile Devices in the Enterprise, NIST SP 800-124 Rev. 2, May 2023
- **Directive-Type Memorandum (DTM) 17-007 –"Interim Policy and Guidance for Defense Support to Cyber Incident Response," Incorporating Change 6, June 21, 2023**

OTHER INFRASTRUCTURES FROM CISA LISTING OF CRITICAL INFRASTRUCTURE SECTORS https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Communications: Sector-Specific Agency: Department of Homeland Security. "The private sector is primarily responsible for protecting sector infrastructure and assets. CISA helps the private sector predict, anticipate, and respond to sector outages." https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/communications-sector The Communications Sector is closely linked to other sectors, including:

- The Energy Sector, which provides power to run cellular towers, central offices, and other critical communications facilities and also relies on communications to aid in monitoring and controlling the delivery of electricity.
- The Information Technology Sector, which provides critical control systems and services, physical architecture, and Internet infrastructure, and also relies on communications to deliver and distribute applications and services.
- The Financial Services Sector, which relies on communications for the transmission of transactions and operations of financial markets.
- The Emergency Services Sector, which depends on communications for directing resources, coordinating response, operating public alert and warning systems, and receiving emergency 9-1-1 calls.
- The Transportation Systems Sector, which provides the diesel fuel needed to power backup generators and relies on communications to monitor and control the flow of ground, sea, and air traffic.

From the **Communications Sector-Specific Plan, 2015 (An Annex to the NIPP 2013).** This plan is designed to "guide the sector's voluntary, collaborative efforts to improve security and resilience over the next four years. " The sector's goals and priorities are:



Sector Goals	Joint Sector Priorities
1 **Protect and enhance the overall physical and logical health of communications.**	**Cyber and Physical Security**: Coordinate with public and private sector partners regarding cyber and physical security information and trends, strategies, initiatives, programs, and best practices. **Future State**: Enhanced cyber and physical risk identification and management capabilities through the use of existing programs.
2 **Rapidly reconstitute critical communications services in the event of disruption and mitigate cascading effects.**	**Resilience**: Promote and coordinate efforts to improve communications resilience by public and private sector partners before, during, and after incidents affecting communications. **Future State**: Enhanced sector programs and initiatives that increase sector-wide incident response and recovery capabilities.
3 **Improve the sector's national security and emergency preparedness (NS/EP) posture with Federal, State, local, tribal, international, and private sector entities to reduce risk.**	**Dependencies and Interdependencies**: Coordinate identification of sector dependencies and interdependencies with public and private sector partners and implement appropriate mitigation actions to make critical infrastructure more resilient and less vulnerable to manmade or natural threats. **Future State**: Improved ability to identify cross-sector dependencies and interdependencies and develop sector-wide risk mitigations strategies to address them.
	Partnership and Engagement: Coordinate with public and private sector partners regarding critical infrastructure security and resilience information, trends, strategies, initiatives, programs, and best practices. **Future State**: Advanced outreach and awareness programs that communicate sector-developed risk management and mitigation practices and strategies with sector stakeholders.

These are amplified throughout the document, along with risk management approaches and measures processes.

.

Energy: **Sector-Specific Agency: Department of Energy.** "The energy sector protects a multifaceted web of electricity, oil, and natural gas resources and assets to maintain steady energy supplies and ensure the overall health and wellness of the nation."

"The Energy Sector is well aware of its vulnerabilities and is leading a significant voluntary effort to increase its planning and preparedness. Cooperation through industry groups has resulted in substantial information sharing of best practices across the sector. Many sector owners and operators have extensive experience abroad with infrastructure protection and have more recently focused their attention on cybersecurity." **https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/** For the Communications Sector, q.v., the Energy Sector "provides power to run cellular towers, central offices, and other critical communications facilities and also relies on communications to aid in monitoring and controlling the delivery of electricity."

From the **Energy Sector-Specific Plan, 2015.** **https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf**

The **National and Energy Sector Critical Infrastructure Goals** (p.3) are:

- Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities.
- Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, Energy Sector-Specific Plan 2015 4 while accounting for the costs and benefits of security investments.

- Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, as well as effective responses to save lives and ensure the rapid recovery of essential services.
- Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making.
- Promote learning and adaptation during and after exercises and incidents.

the **Electricity Subsector Priorities** are:

Tools and Technology—Deploying tools and technologies to enhance situational awareness and security of critical infrastructure. • Deploying proprietary government technologies on utility systems that enable machine-to-machine information sharing and improved situational awareness of threats to the grid. • Implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Information Flow—Making sure actionable intelligence and threat indicators are communicated between the government and industry in a time-sensitive manner. • Improving the bidirectional flow of threat information. • Coordinating with interdependent sectors.

Incident Response—Planning and exercising coordinated responses to an attack. • Developing playbooks and capabilities to coordinate industry-government response and recovery efforts. • Ongoing assessments of equipment-sharing programs.

Information Technology: **Sector-Specific Agency: Department of Homeland Security.** "The nation's growing dependency on IT makes the Information Technology Sector mission – to identify and protect against cyber threats and vulnerabilities - more complex and important every day." https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/information-technology-sector For the Communications Sector, q.v., the IT Sector provides: "critical control systems and services, physical architecture, and Internet infrastructure, and also relies on communications to deliver and distribute applications and services."

From the **IT Sector-Specific Plan 2016 (An Annex to the National Infrastructure Protection Plan 2013).**

https://www.cisa.gov/sites/default/files/2023-01/nipp-ssp-information-technology-2016-508%20%281%29.pdf

The IT Sector's vision is to "To achieve a sustained reduction in the impact of incidents on the Sector's critical functions." (p. 9). The ITSSP's intent is "to guide the Sector's voluntary, collaborative efforts to improve security and resilience over the next four years." The sector's six critical functions are:

7. Provide IT products and services;
8. Provide incident management capabilities;
9. Provide domain name resolution services;
10. Provide identity management and associated trust support services;
11. Provide Internet-based content, information, and communications services; and
12. Provide Internet routing, access, and connection services.

Figure 2-1 (p. 3) describes these functions in more detail. The emergence of the IoT and the growing importance of cyber-physical systems are mentioned, along with the growth of social networking, but artificial intelligence is not. Other sections of the plan outline IT functions, risks, and mitigations; Critical Infrastructure Partners (public, private, and international); risk assessment and mitigation; R&D opportunities; and metrics. Cybersecurity is emphasized throughout, as are partnerships.

Emergency Services: Sector-Specific Agency: Department of Homeland Security. "Supporting millions of skilled personnel with physical and cyber resources, the Emergency Services Sector helps save lives, protect property and the environment, and assist in recovery efforts." **https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/emergency-services-sector**

Five distinct disciplines compose the ESS, encompassing a wide range of emergency response functions and roles:

- Law Enforcement
- Fire and Rescue Services
- Emergency Medical Services
- **Emergency Management**
- Public Works

The ESS also provides 11 different kinds of specialized emergency services through individual personnel and teams.

From the Emergency Services Sector-Specific Plan 2015 (An Annex to the NIPP 2013).
https://www.cisa.gov/sites/default/files/publications/emergency-services-sector-specific-plan-112015-508.pdf

The Emergency Services Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) have identified four goals:

- Partnership Engagement—Continuous growth and improvement of sector partnerships, which enable the sector to effectively sustain collaborative dialogues to address risk mitigation and resilience efforts within the sector.
- Situational Awareness—Support an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant sector information, intelligence, and incident reporting.
- Prevention, Preparedness, and Protection—Employ a risk-based approach to improve the preparedness and resilience of the sector's overall capacity to perform its mission through targeted decisions and initiatives.
- Recovery and Reconstitution—Improve the operational capacity, sustainability, and resilience of the sector and increase the speed and efficiency of restoration of normal services and activity following an incident.

Within these are 12 priorities and 18 activities for collaboration.

Interdependencies with other sectors are:

- Energy—Fuel and electric power are essential for ESS operations and the ability of critical infrastructure to respond to emergencies.

- Communications—Radio spectrum networks and infrastructure enable ESS to carry out its mission.
- Transportation Systems—Secure and effective movement of goods and personnel over multiple modes is required for emergency response and recovery.
- Water—Water is critical for sustaining communities and infrastructure before, during, and after emergencies.
- Healthcare and Public Health—First responders and EMS coordinate with the Healthcare Sector to respond to emergencies.
- Information Technology—A variety of cyber-related assets, systems, and disciplines are increasingly essential to help ESS carry out its mission.

Sector resources include the following publications

- **Emergency Services Sector Profile, 2021 https://www.cisa.gov/sites/default/files/2023-02/emergency-services-sector-profile_12-2022_508_1.pdf**
- **Emergency Services Sector Landscape, 2019. https://www.cisa.gov/sites/default/files/2023-04/emergency-services-sector-landscape_082019_508.pdf**
- **Emergency Services Sector-Specific Tabletop Exercise Program 2014 (available on HSIN) https://www.cisa.gov/sites/default/files/2023-04/emergency-services-sector-landscape_082019_508.pdf**
- **Emergency Services Sector Continuity Planning Suite, revised 2021. https://www.cisa.gov/sites/default/files/2023-04/emergency-services-sector-landscape_082019_508.pdf**

Transportation Systems: **Co-Sector-Specific Agencies: Department of Homeland Security and Department of Transportation.** “Moving millions of people and goods across the country every day, CISA protects the transportation systems sector from a limitless number of threats and risks to ensure a continuity of operations.” https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector

The Transportation Systems Sector consists of seven key subsectors, or modes:

- Aviation
- Highway and Motor Carrier
- Maritime Transportation System
- Mass Transit and Passenger Rail
- Pipeline Systems
- Freight Rail
- Postal and Shipping

For the purpose of addressing cross-sector, cascading infrastructure disruptions, the principal interactions will most affect highways in that the restoration of most damaged comms and power capabilities will require road access by repair crews.

From the Transportation Systems Sector-Specific Plan (TS SSP), 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf "The TS SSP is a planning tool for the SSAs, critical infrastructure owners and operators, and partners at the regional, State, local, tribal, and territorial levels [it] is intended to focus the resources and programming of agencies and companies on collaboratively determined priorities for effective management of sector risks. It is not intended to replace agency- or company-specific planning documents or risk management processes.

The TS SSP identifies the following goals: (p. 2)

- Goal 1: Manage the security risks to the physical, human, and cyber elements of critical transportation infrastructure.
- Goal 2: Employ the Sector's response, recovery, and coordination capabilities to support whole community resilience.
- Goal 3: Implement processes for effective collaboration to share mission-essential information across sectors, jurisdictions, and disciplines, as well as between public and private stakeholders.
- Goal 4: Enhance the all-hazards preparedness and resilience of the global transportation system to safeguard U.S. national interests.

Cyber technologies upon which transportation services rely include positioning, navigation, tracking, shipment routing, industrial system controls, access controls, signaling, communications, and data and business management. These technologies are often interconnected through networks and remote access terminals, which may allow malicious actors easier access to key nodes. Continuity of operations and system resilience following a disaster are increasingly dependent on the recovery of cyber systems. (p. 11)