CISA
CYBER+INFRASTRUCTURE

A Guide to

Critical Infrastructure Security and Resilience

November 2019

Table of Contents

Table of Contents 2
Foreword 3
What is Critical Infrastructure? 4
What are the "Threats and Hazards" to Critical Infrastructure? 6
Who is Responsible for Critical Infrastructure? 9
What Drives Critical Infrastructure Security and Resilience? 11
Getting Started 13
The Risk Management Framework 15
The Role of Risk Assessments 17
Training and Education 19
Evaluating the Program 20
Promoting the Program 21
Conclusion 22

Foreword

In the United States (U.S.), the Patriot Act of 2001 defined critical infrastructure as those "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."

As stated in the National Infrastructure Protection Plan (NIPP) *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, the U.S. vision is:

> *A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.* This vision drives the basic approach to critical infrastructure security and resilience in the United States, to: *Strengthen the security and resilience of the Nation's critical infrastructure, by managing physical and cyber risks through the collaborative and integrated efforts of the critical infrastructure community.*

The U.S. Department of Homeland Security, in collaboration with the U.S. Department of State, has prepared this guide to serve as an overview of the approach to critical infrastructure security and resilience adopted in the United States. As attacks on soft targets and crowded places continue across the globe, the need to address current and emerging challenges increases. Therefore, the Department of Homeland Security and Department of State are working together to enhance domestic and global security, with ongoing programs, and recognizing that new approaches may be needed to address these evolving issues.

The intent of this guide is to share basic information and U.S. lessons learned over the last 15 years, rather than to promote specific approaches. This information may apply to other countries, particularly those countries that are considering developing or refining their own voluntary and regulatory-based infrastructure security and resilience programs.

Each section of this guide provides additional resources for more detailed information on the specific topics covered. The referenced websites also contain many other useful resources. Readers are encouraged to explore this information as well.

Brian Harrell
Assistant Director for Infrastructure Security
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

Ambassador Nathan Sales
Coordinator for Counterterrorism
Bureau of Counterterrorism
U.S. Department of State

What is Critical Infrastructure?

Critical infrastructure includes the assets, systems, facilities, networks, and other elements that society relies upon to maintain national security, economic vitality, and public health and safety. We know critical infrastructure as the power used in homes, the water we drink, the transportation that moves us, the stores where we shop, and the Internet and communications we rely on to maintain our contact with friends, family, and colleagues. In the U.S., this physical and cyber infrastructure is typically owned and operated by the private sector, though some is owned by federal, state, or local governments. Not all infrastructure within an industry sector is critical to a nation or region. It is necessary to identify which infrastructure is both critical to maintain continued services or functions and vulnerable to some type of threat or hazard. Prioritizing the allocation of available resources to that subset of infrastructure can enhance a nation's security, increase resiliency, and reduce risk.

There are four designated lifeline functions – transportation, water, energy, and communications, which means that their reliable operations are so critical that a disruption or loss of one of these functions will directly affect the security and resilience of critical infrastructure within and across numerous sectors. For example, energy stakeholders provide essential power and fuels to stakeholders in the communication, transportation, and water sectors, and, in return, the energy sector relies on them for fuel delivery (transportation), electricity generation (water for production and cooling), as well as control and operation of infrastructure (communication).

These connections and interdependencies between infrastructure elements and sectors mean that the loss of one or more lifeline function(s) typically has an immediate impact on the operation or mission in multiple sectors. As a result, additional loss of other functions may arise over time. Further, identifying and officially recognizing industry sectors that are lifeline sectors and/or have cross-sector interdependencies facilitates collaboration and information exchange that promotes continuity of operations and services. The choice of sectors prioritized in outreach efforts should reflect an understanding of the infrastructure's interconnectedness and interdependencies, recognize existing industry associations, and align to government agencies' roles and oversight responsibilities.

Critical infrastructure encompasses functions in addition to the lifelines. For example, in 2017, Election Infrastructure was designated a subsector of the Government Facilities Sector due to the importance of free and fair democratic elections as a foundation of the American way of life. Working to reduce risk in partnership with the public and private sector entities responsible for providing this kind of critical function is a crucial element of maintaining public confidence in the Nation's critical infrastructure.

Current U.S. Critical Infrastructure Sectors

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

Selected Resources

1. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act OF 2001* (https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf)
2. The U.S. Department of Homeland Security Cybersecurity and Infrastructure Agency webpage. (https://www.cisa.gov/)
3. NIPP 2013: *Partnering for Critical Infrastructure Security and Resilience* (https://www.cisa.gov/national-infrastructure-protection-plan)
4. The U.S. Energy Sector-Specific Plan outlines generic cross-sector interdependencies in Section 4.2, "Interdependency and Coordination," and provides a high-level overview of interdependencies among the lifeline functions. (https://www.cisa.gov/infrastructure-security)
5. The DHS Critical Infrastructure Security webpage contains additional information. (https://www.dhs.gov/topic/critical-infrastructure- security)

What are the "Threats and Hazards" to Critical Infrastructure?

Both natural and man-made (deliberate or accidental) incidents have the potential to harm, damage, incapacitate, or destroy critical infrastructure. Rather than focusing on one type of threat or hazard at a time, such as hurricanes or terrorism, States should identify all threats and hazards that pose the greatest risks to critical infrastructure, which allows for more effective and efficient planning and resource allocation.

Critical infrastructure has long been subject to risks associated with physical threats and natural disasters, and is also now increasingly exposed to cyber risks. These risks stem from a growing integration of information and communications technologies with critical infrastructure and adversaries focused on exploiting potential cyber vulnerabilities. As physical infrastructure becomes more reliant on complex cyber systems for operations, critical infrastructure can become more vulnerable to certain cyber threats, including transnational threats.

Connections and interdependencies between infrastructure elements and sectors means that damage, disruption, or destruction to one infrastructure element can cause cascading effects, impacting continued operation of another. Identifying and understanding interdependencies (two-way) or dependencies (one-way) between infrastructure elements and sectors are important for assessing the risks and vulnerabilities and for determining which steps may be taken to increase security and resilience. For example, the electric grid relies on integrated information and communication systems from other critical infrastructure sectors in order to operate. One example of the immediate need for energy is in recovery operations following a natural disaster. Until the energy system is restored, water and wastewater systems cannot provide clean water, natural gas cannot flow to provide heat, and generation and telecommunications systems quickly become inoperative once backup power sources begin to fail. Energy is so critical to U.S. reconstitution and recovery efforts that Florida Power and Light (FPL) invested close to $3 billion over the past several years to rebuild and strengthen the energy generation and provision infrastructure within Florida. The money paid for strengthening 700 power lines to critical facilities such as police stations, hospitals and gas stations; burying 60 power lines underground; clearing vegetation from 150,000 miles of lines; inspecting 150,000 poles per year; and installing 4.9 million smart meters to help predict and prevent power outages. After hurricanes ravaged the entire state in 2017, FPL was able to get power back up to all customers capable of safely receiving power within days, including emergency services, hospitals and other life-sustaining critical infrastructure.

Soft Targets and Crowded Places

From cyber to physical security threats, we live in a world where terrorist activity is increasing and becoming more diffuse, where attacks can be either simple and opportunistic in nature or complex and organized. The rising number of attacks against soft targets/crowded places in multiple cities worldwide from Orlando to New Zealand, San Bernardino to Sri Lanka, demonstrates that the nature of the threat is evolving and reinforces the need for global vigilance, preparedness, and collaboration. National and international efforts seek to address the trend toward attacking soft targets and crowded places.

For example, the United States is working domestically with all levels of government to provide training, resources, and materials to enhance and promote soft target and crowded places security.

On the international front, countries are working together to share good practices, lessons learned and experiences on attacks against soft targets and crowded places to help create and advance a global culture of security. The Global Counterterrorism Forum (GCTF) Soft Target Protection Initiative, co-led by the United States and Turkey, involved a series of regional workshops in 2017 with government and the private sector aimed at raising awareness, increasing preparedness, and creating the first set of non-binding international good practices on soft target protection in a counterterrorism context.

The good practices are meant to inform and guide governments and private industry as they work together to develop policies, practices, guidelines, programs, and approaches in protecting their citizens from terrorist attacks on soft targets and crowded places. Discussions acknowledged that States have the primary responsibility for ensuring security in their territory and protecting their civilians in accordance with the United Nations (UN) Charter. The UN Security Council Resolution 2341 (2017) outlines the role of States on the protection of critical infrastructure and particularly vulnerable targets, such as public places, from terrorist attacks, including through public-private partnerships as appropriate.

Threats and Hazards

Threats and hazards may be specific to geographic regions, or across an entire country, and may even have global ramifications; such as:

- **Climatological Events** (extreme temperatures, drought, wildfires)
- **Hydrological Events** (floods)
- **Meteorological Events** (tropical cyclones, severe convective storms, severe winter storms)
- **Geophysical Events** (earthquakes, tsunamis, volcanic eruptions)
- **Pandemics** (global disease outbreaks)
- **Space Weather Events** (geomagnetic storms)
- **Technological and Industrial Accidents** (structural failures, industrial fires, hazardous substance releases, chemical spills)
- **Unscheduled Disruptions** (aging infrastructure, equipment malfunction, large scale power outages)
- **Criminal Incidents and Terrorist Attacks** (vandalism, theft, property damage, active shooter incidents, kinetic attacks)
- **Cyber Incidents** (denial-of-service attacks, malware, phishing)
- **Supply Chain Attacks** (exploiting vulnerabilities to cause system or network failure)
- **Foreign Influence Operations** (to spread misinformation or undermine democratic processes)
- **Untrusted Investment** (to potentially give foreign powers undue influence over American critical infrastructure)

These threats and hazards must be analyzed to determine their potential impacts on infrastructure and how likely they are to occur.

Managing Cross-Sector Risk to Critical Infrastructure

In April 2019, Cybersecurity and Infrastructure Security Agency (CISA) released the first-ever set of 55 National Critical Functions to more effectively manage the most strategic risks to the nation. National Critical Functions are the functions of government and the private sector so vital to the United States 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. The functions were developed in coordination with sector and state, local, tribal and territorial partners, and enable the critical infrastructure community to analyze complex challenges that cannot be easily identified, understood, or examined within the existing risk management structures for cyber and physical infrastructure.

Effective risk management depends on the critical infrastructure community's ability to engage across sectors to facilitate a shared understanding of risk and integrate a wide range of activities to manage risk. As a framework, the National Critical Functions captures cross-cutting, cross-sector risks and associated dependences that may have cascading impacts within and across sectors. By identifying what is truly critical at the functional level and where key dependencies and interdependencies lie, CISA can identify pockets of risk that are deemed unacceptable to the nation. This approach will allow CISA to more effectively capture risks to supply chain security and resilience, such as the introduction of counterfeit parts and components or the unique challenges of lean processes and just-in-time practices. The National Critical Functions framework also allows CISA to more effectively assess major cybersecurity issues, such as attacks conducted to steal intellectual property, or the abuse of control systems that could lead to physical damage, personnel hazards, and interrupted operations. The functional approach also highlights the systemic challenges of workforce development in the face of rapid technology growth. Finally, the National Critical Functions signal a recognition that technology is driving a need for coordination and collaboration that builds on the legacy successes of the sector approach, allowing for cross-industry engagement around complex challenges like vulnerabilities associated with position, navigation, and timing systems.

For more information see: www.cisa.gov/national-critical-functions.

Selected Resources

1. The Department of Homeland Security Critical Infrastructure Sectors (https://www.cisa.gov/critical-infrastructure-sectors)
2. "Critical Infrastructure, Interdependencies, and Resilience" by T.D. O'Rourke in *The Bridge* (https://www.nae.edu/7655/ CriticalInfrastructureInterdependenciesandResilience)
3. Florida Public Service Commission (http://www.psc.state.fl.us/ElectricNaturalGas/EnergyInfrastructure)
4. The Department of Homeland Security Securing Soft Targets and Crowded Places home page (https://www.cisa.gov/securing-soft-targets-and-crowded-places)
5. *The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation* provides an overview of many types of threats and hazards (https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf)
6. *The Insider Threat to Critical Infrastructures* (https://www.dhs.gov/cisa/insider-threat-mitigation)
7. *The Department of Homeland Security Soft Targets and Crowded Spaces Resource Guide and Security Plan Overview:* Many of the materials in this guide were created in collaboration with industry partners to ensure they are useful and reflective of the dynamic environment we live in. (https://www.cisa.gov/publication/securing-soft-targets-and-crowded-places-resources)
8. United Nations Security Council Resolution 2341 on Protection of Critical Infrastructure (http://www.un.org/en/ga/search/view_doc.asp?symbol=S/ RES/2341%282017%29&referer=/english/&Lang=E)
9. GCTF Soft Target Protection Initiative Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism Context (http://www.un.org/en/ga/ search/view_doc.asp?symbol=S/RES/2341%282017%29&referer=/english/&Lang=E)
10. United Nations: recommended practices for the protection of critical infrastructure (https://www.thegctf.org/Portals/1/Documents/Links/ Meetings/2017/Twelfth GCTF Coordinating Committee Meeting/GCTF - Antalya Memorandum on the Protection of Soft Targets in a Counterterrorism)
11. United Nations Compendium: Protecting CI from Terrorist Attacks: https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf.

Who is Responsible for Critical Infrastructure?

Strengthening the security and resilience of critical infrastructure is a shared responsibility between stakeholders — the critical infrastructure owners and operators, and the various government entities and non-government organizations (including industry associations).

Roles and responsibilities for maintaining or improving the security and resilience of infrastructure vary widely and are affected by many factors such as:

- Public versus private ownership;
- Regulations within a sector;
- Anticipated threats and hazards to a specific sector; and
- Decisions on whether the sector or region chooses to focus on taking actions to protect infrastructure, reduce consequences, or rapidly respond to and recover from adverse events.

Industry associations often play a key role in recommending practices, while in other sectors there may be regulations that require certain actions — or both may apply. Some sectors have statewide or national design standards that help protect against damage from events like fires, floods, and earthquakes. Insurance providers may also impose security requirements on their policyholders in some sectors. The U.S. chemical sector for instance, promotes preparedness through a voluntary framework between industry and government, and is partially subject to regulatory programs.

Response efforts may be driven by first responders, owners/operators, or regional and federal resources, but responsibility for recovery in a predominately voluntary system, such as in the U.S., generally falls to the owners and operators who know the infrastructure best.

Engagement at all levels of government and industry fosters mutual understanding and trust, and promotes information sharing and practical exchanges. Engagements that promote planning, prioritization of resources, exercises, and training greatly contribute to the success of national preparedness efforts and, especially, effective and timely responses. Such engagements also galvanize support for joint public-private efforts.

Case Study - Information Sharing and Analysis Centers

Information Sharing and Analysis Centers (ISACs) help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs are trusted entities established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats and mitigation. The concept of ISACs was introduced and promulgated pursuant to Presidential Decision Directive-63 (PDD-63), signed in 1998. Some ISACs formed as early as 1999, and most have been in existence for at least ten years. Typically, nonprofit organizations, ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.

The Real Estate Information Sharing and Analysis Center (RE-ISAC) serves as an excellent example of this information sharing construct. The RE-ISAC a public-private information sharing partnership between the U.S. Commercial Facilities Sector and federal homeland security officials organized and managed by The Real Estate Roundtable (non-profit public policy organization based in Washington, DC). The Commercial Facilities Sector is an integral part of U.S. critical infrastructure and includes a vast range of sites where people live, work, shop and play. The RE-ISAC is the designated sector-specific conduit for sharing information about potential physical and cyber security threats and vulnerabilities to help protect commercial facilities and the people who use them. By bringing together industry representatives to aggregate, share and assess information, the quality, relevance, and overall value of the resulting information increases exponentially. As a result, the RE-ISAC and its members are able to achieve objectives that no single industry organization could accomplish alone. This benefits the industry, government and the nation as a whole.

Voluntary and Regulatory Approaches

Infrastructure security and resilience programs can be voluntary, regulatory, or a combination of both. In the United States, voluntary programs are most common.

- Voluntary programs work best to promote new programs or where the diversity within the industry is too great to apply common standards.
- Voluntary programs must have strong value propositions or business cases to demonstrate the benefits of participation, to ultimately be successful.
- Regulatory approaches may be desired to ensure a common standard is required of all, to promote certain industry practices, where appropriate, and to ensure compliance is not a competitive disadvantage.

Selected Resources

1. See the FEMA A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action website (http://www.fema.gov/whole-community)
2. The DHS Critical Infrastructure Sector Partnerships web page (https://www.cisa.gov/critical-infrastructure-sector-partnerships)

What Drives Critical Infrastructure Security and Resilience?

Security may be defined as reducing the risk to critical infrastructure from intrusions, attacks, or the effects of natural or man-made disasters, through the application of physical means or defensive cyber measures.

Resilience may be defined as the ability to prepare for and adapt to changing conditions. This means being able to withstand and recover rapidly from disruptions, deliberate attacks, accidents, or naturally-occurring threats or incidents. Resilient infrastructure must also be robust, agile, and adaptable.

A strong critical infrastructure security and resilience program is based on collaboration and information sharing.

Collaboration is facilitated by establishing the structures and processes necessary for government(s) and the private sector to communicate freely without releasing proprietary information or providing unfair advantage; support a trusted information sharing environment where stakeholders share information to strengthen security and resilience; and ensure relevant stakeholders are fairly represented and engaged, from all levels of government, industry, emergency management, and security.

Successful information sharing requires established mechanisms or channels to reach stakeholders regularly, as well as before, during, and after an incident. Sharing information can take many forms, including training events, briefings, email alerts, conference calls, or meetings in secure locations to discuss classified materials about specific threats or hazards, and documents and forums that encourage sharing lessons learned. The latter category improves the planning for handling future events.

To facilitate voluntary collaboration and information sharing within and across critical infrastructure sectors and government agencies (federal, state, local, tribal, and territorial), the U.S. has established a formal partnership framework comprised of government and private sector coordinating councils that meet separately as well as jointly to enhance critical infrastructure security and resilience. Private sector information sharing is conducted through Information Sharing and Analysis Centers (ISACs). ISACs primarily operate through a sector-based model, meaning that organizations within a certain critical infrastructure sector (or a specific segment within a sector) join together to share information. Although many of these groups are already essential drivers of effective information sharing, some organizations do not fit neatly within an established sector or have unique needs. The U.S. also has industry collaborative Information Sharing and Analysis Organizations (ISAOs). Created to gather, analyze, and disseminate cyber threat information, ISAOs offer a more flexible approach to self-organized information sharing activities amongst specific communities of interest (for example, small businesses across sectors such as legal, accounting, and consulting firms that support cross-sector clients).

Information Sharing

The following can help facilitate and support information sharing efforts:

- Identify stakeholders who have an interest and/or stake in critical infrastructure security and resilience.
- Provide actionable threat information so that owners/operators can implement plans and take appropriate action.
- Recognize that information sharing must be reciprocal – as owners and operators may each observe suspicious activity that helps identify and validate threats.
- Establish and maintain user-friendly information sharing systems for stakeholders to promote routine as well as rapid communication during events/emergencies.
- Threat information should be processed to remove the specifics of data sources and collection methods, so it can be shared more broadly, particularly with relevant stakeholders.
- Owner and operator information must be protected, in accordance with national legislation.

Selected Resources

1. The *Critical Infrastructure Threat Information Sharing Framework: A Resource Guide* describes how threat information is shared between the federal government and owners and operators. This framework includes descriptions and contact information for key threat information-sharing entities, as well as case studies that show how threat information sharing works in practice. (https://www.cisa.gov/publication/ci-threat-info-sharing-framework)
2. Information Sharing and Analysis Organizations (https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos)
3. Both of the U.S. information sharing mechanisms – the Infrastructure Protection Gateway and the Homeland Security Information Network (HSIN) are used to reach and connect critical infrastructure partners; similar networks may be of use in other countries to provide a shared platform for gathering, analyzing, and reporting information on potential threats and hazards and to maintain situational awareness.

Getting Started

Developing a critical infrastructure security and resilience program starts by establishing goals and objectives; these may be at a national, regional, local, sector, or organizational level. Vision and mission statements may also be helpful to share the view of what the program seeks to accomplish. The steps identified in the following page are generally documented in a critical infrastructure security and resilience plan. To keep the effort moving and to ensure plans are not sidelined by other priorities, having specific deadlines and milestones is important.

In some countries, a top-down or national framework may be useful to guide and unify efforts, including those between government and industry. However, in other countries, it may be more common for states, provinces, regions, or similar entities to organize and oversee security, emergency management, and preparedness efforts.

A critical infrastructure security and resilience program should reflect the existing operational environment, and cultural values/ beliefs, and build upon existing relationships, efforts, and policies. It should align with and support other programs so that resources are effectively utilized, existing capabilities and communities leveraged, and roles and responsibilities are understood.

Determining the scope of the effort is also important when starting out. Some questions to answer include: whether to identify a few lifeline sectors or a larger group of infrastructure sectors? Public and private infrastructure, or just one of these to start? Will there be any funding for the establishment of the program, or will there be a government directive to get work underway? Are all threats and hazards to be included (recommended) or just selected ones? The more comprehensive and integrated the scope, the greater the preparedness benefits that can be realized on an ongoing basis.

Other initial questions to ask relate to identifying stakeholders — which agencies, associations, infrastructure owners and operators, and other stakeholders should be involved? Experience in the U.S. suggests that broad-based participation is key to the successful development and implementation of a comprehensive program to promote continuous improvement in security and resilience.

Identifying the roles and responsibilities of different stakeholders at the beginning can help align and even combine relevant expertise/disciplines, focus efforts, ensure that timelines are met, and provide the desired inputs for an effective program.

Similarly, identifying existing programs or efforts that relate to infrastructure security and resilience can help anchor the development of an overall program and serve as a guide to other sectors. Consider if there are airport screening projects or water and energy security efforts underway or already in place that can serve as examples.

Collaboration and information sharing across the critical infrastructure community are fundamental to the overall process. Establishing mechanisms that foster open collaboration and ensure the exchange of timely and actionable information as well as best practices will help gain participation in the program — both as the program is designed and developed and when it is implemented. Collaborative partnerships enable more effective and efficient risk management. Consider the need for these mechanisms and partnerships at each level of organization or governance, for example, within and across sectors, within and across government, and within and across the private sector.

Basic Steps for a Critical Infrastructure Security and Resilience Plan

- Establish goals and objectives
- Identify existing examples of relevant critical infrastructure security and resilience plans or programs
- Determine the scope
- Identify the stakeholders
- Document roles and responsibilities
- Establish coordination and information sharing mechanisms
- Set timelines
- Build a risk management framework
- Design and conduct assessments
- Conduct training and education, including exercises
- Establish metrics
- Promote the program through outreach and awareness

Once you make your plan, be sure to exercise it regularly. Doing so will ensure that, if there is a real-life incident, everyone will know their role and what to do.

Selected Resources

1. In addition to the model in the 2013 NIPP and its predecessors, a model of a city resilience program is the Charleston Resilience Network. (http://www.charlestonresilience.net/)

The Risk Management Framework

Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood — a function of threats and vulnerabilities — and the associated consequences. Risk management is the process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost.

Risk management focuses resources on those threats and hazards that are most likely to cause significant, unwanted outcomes to a specific infrastructure or sector and informs actions designed to prevent or mitigate the effects of those incidents. It also increases security and strengthens resilience by identifying and prioritizing actions to ensure continuity of essential functions and services and support enhanced response and restoration. Risk management facilitates decision making and the setting of priorities across all stakeholders.

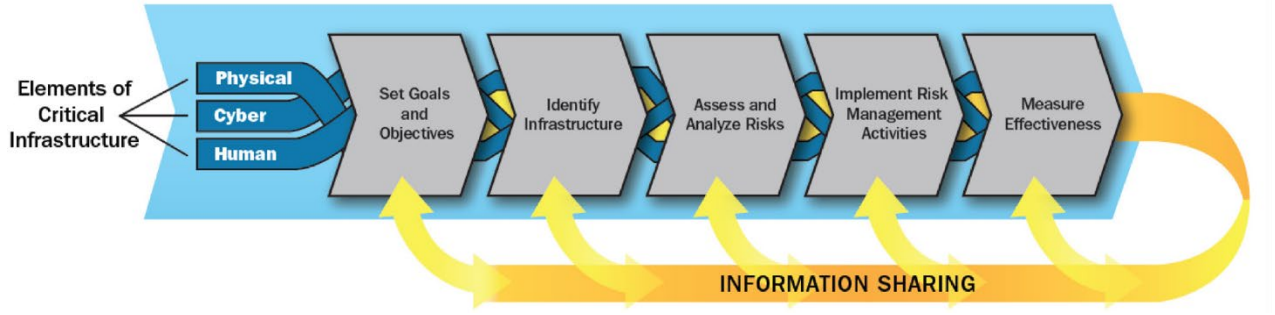
A risk management framework sets out an approach to consistently:

- Identify, analyze, and allocate resources to deter, detect, disrupt, and prepare for threats and hazards to critical infrastructure;
- Prioritize vulnerability reduction efforts, address physical features or operational attributes that make an infrastructure element open to exploitation or susceptible to a given hazard; and
- Mitigate the potential consequences of incidents proactively, or prepare to mitigate them effectively if they do occur.

The risk management framework can be applicable to all levels of government or private sector organizations. It should cover all threats and hazards and varying factors across critical infrastructure sectors, in addition to individual assets and systems.

The current U.S. Critical Infrastructure Risk Management Framework is provided below and described in the National Infrastructure Protection Plan (NIPP) 2013.

U. S. Critical Infrastructure Risk Management Framework



Core U.S. Risk Management Tenets

1. Risk should be identified and managed in a coordinated way within the critical infrastructure community to enable effective resource allocation.

2. Critical infrastructure partnerships can greatly improve understanding of evolving risk to both cyber and physical systems and assets, and can offer data and perspectives from various stakeholders.

3. Understanding and addressing risks from cross-sector dependencies and interdependencies is essential to enhancing overall critical infrastructure security and resilience.

4. Gaining knowledge of and reducing infrastructure risk requires information sharing across all levels of the critical infrastructure community.

5. A partnership approach, involving public and private stakeholders, recognizes the unique perspectives and comparative advantages of the diverse critical infrastructure community. For example, Emergency Support Function 14 of the National Response Framework supports the coordination of cross-sector operations, including stabilization of key supply chains and Community Lifelines, among infrastructure owners and operators, businesses, and their government partners.

6. Regional, state, and local partnerships are crucial to developing shared perspectives on gaps and improvement actions.

7. Critical infrastructure transcends national boundaries, requiring bilateral, regional, and international collaboration; capacity building; mutual assistance; and other cooperative agreements. For example, the "Canada-U.S. Action Plan for Critical Infrastructure" sets the foundation for cross-border critical infrastructure security and resilience efforts between the two countries.

8. Security and resilience should be considered during the design of infrastructure elements.

Selected Resources

1. Tools and Resources to Help Businesses Plan, Prepare, and Protect from an Attack (https://www.cisa.gov/hometown-security)
2. The *Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level* is used at the state, local, and regional levels, to tailor the national approach to fit their respective needs. (https://www.dhs.gov/xlibrary/assets/nipp_srtltt_guide.pdf).
3. Overview of ESF and Support Annexes Coordinating Federal Assistance in Support of the National Response Framework. (https://www.fema.gov/media-library-data/20130726-1825-25045-8535/overview_esf___support_annexes_2008.pdf).

The Role of Risk Assessments

A range of methodologies are available to assess threats and hazards and to guide the development of risk management programs. Assessments help government officials and owners and operators to understand potential incidents and how they could affect infrastructure and communities.

Risk assessments give decision makers better information to determine which mitigation and risk management measures are most critical and to understand where different types of actions are most suitable. The range of available measures includes: coordination with other stakeholders; provision of additional response or recovery equipment; modifications to infrastructure design; restrictions on operations; hiring and training of staff; among others. Risk assessments also keep the focus from automatically defaulting to rare or worst-case events with extreme consequences, promoting consideration of a range of more likely events, even if they have somewhat lesser, but still significant, consequences.

The objective is to perform accurate and comprehensive assessments that individually or collectively cover threat, vulnerability, and consequence (also known as hazard, frequency, and consequence for non-threat-based risks). The type of assessment may be determined by international standards, industry best practices, or available historical data. As cybersecurity is a key concern for ensuring the resilience of critical infrastructure, a comprehensive understanding of security and resilience involves considerations of both physical and cyber domains in a holistic fashion. Assessments, therefore, should involve experts from both the physical and cybersecurity domains of critical infrastructure. Analyzing dependencies and interdependencies as a part of risk assessments (at international, national, regional, and/or local levels) can further inform planning and facilitate prioritization of resources to ensure the continuity of critical services and mitigate the cascading impacts of incidents that do occur. Modeling and simulation may be an important part of analyzing complex systems and interdependencies. In the U.S., non- governmental entities (academics, associations, etc.) also develop and disseminate products regarding threats, vulnerabilities, and potential consequences to broader audiences.

Performing a risk assessment on an infrastructure element can require a significant expenditure of resources by owners/operators or others which may not be justified in all cases. To determine the scale of the assessment, many risk assessment methodologies suggest that some type of screening – typically a consequence screen to see if potential impacts are significant or not – be performed first. This helps minimize the resources devoted to full risk assessments. In the U.S., the government offers expert guidance and assistance through protective security advisors deployed across the country and provides tools to assist owners and operators in conducting assessments and to help in managing cost.

A full risk assessment may be justified for all or most critical infrastructure elements in certain areas where the potential consequences associated with disruption, destruction, or exploitation are especially high. In these limited cases, a screening process is not necessary as all

of the assets would "screen in." A screening process is recommended for all other infrastructure to help lower the demands on those elements that may not warrant a full assessment. As an example, screening-level assessments may be sufficient for most infrastructure in rural areas, while large metropolitan areas may warrant full risk assessments for a number of infrastructure elements.

Sharing the results of assessments among critical infrastructure stakeholders will provide a greater understanding of the probability, impact, and related consequences of various threats and hazards.

Communicating the assessment results can guide planning and resource allocation and expenditures for relevant stakeholders. In addition, conveying the risk will inform preparedness, mitigation and response efforts undertaken by owners, operators, and government officials.

Informing Catastrophic Earthquake Preparedness in the Pacific Northwest

A magnitude 9.0 Cascadia Subduction Zone earthquake will have a broad, regional impact area that extends more than 700 miles from British Columbia to Northern California. Direct seismic forces, ground failure, and tsunami flooding will extensively damage much of the region's infrastructure at a systemic level. In many cases, these systems are likely to be rendered unusable immediately after the initial earthquake. Such extensive damage to western Washington's infrastructure will place significant demand on the government and private-sector response to provide basic commodities and relief supplies into the region to sustain disaster survivors. Understanding with greater clarity the scope, scale, and degree of a CSZ earthquake on critical infrastructure assets and systems while accounting for system level resilience attributes is then a vital step in informing disaster response and recovery plans and pre-disaster mitigation efforts. In support of such Federal, state, and local CSZ preparedness efforts, the CISA Regional Resiliency Assessment Program (RRAP) has undertaken three collaborative regional resilience assessment projects focusing on regional transportation systems—including road, rail, bridge, maritime, and aviation modes—and water supply in the states of Washington and Oregon. To date, these efforts have:

- Identified the most viable multi-modal transport route and facilities that could be utilized in the CSZ response.
- Identified and prioritized transportation routes and facilities for potential investments in hardening/maintenance, replacement/retrofitting, and/or mitigation measures.
- Provided replicable seismic vulnerability screening methodologies for further use by State and local authorities.
- Examined the seismic vulnerability and role of airfields in enabling delivery of life-sustaining resources to affected areas.
- Begun identifying probable water system impacts and potential alternative water sources and watering strategies for survivors.

Most importantly, the collaborative nature of these efforts has brought together and fostered even greater cooperation between Federal, state, and local agencies and the private sector on these critically-important issues in which each has a distinct but essential role. This important work is directly influencing disaster planning and readiness, improving the resilience of critical infrastructure and, with it, the resilience of communities in these two states.

Selected Resources

1. The Infrastructure Protection Gateway is a repository for certain assessment tools. The IP Gateway illustrates how the Government can virtually share tools with partners once they are available. (https://www.cisa.gov/ip-gateway)
2. The Critical Infrastructure Vulnerability Assessments web page describes a number of specific approaches. (https://www.cisa.gov/critical-infrastructure-vulnerability-assessments)
3. An example of an international standard for critical infrastructure is the European Union Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. (https:// eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF)

Training and Education

Training and education are fundamental to the success of a critical infrastructure security and resilience program and must reach government officials, infrastructure owners and operators, first responders, and the public, where appropriate.

Training should be available in many different forms to ensure the broadest reach, including instructor-led courses, webinars, web-based independent study courses, and written guidance and job aids. Training offerings may be on general concepts, best practices, or very specific topics. The sidebar below illustrates the range of topics currently offered by the U.S. Department of Homeland Security and other infrastructure partners.

Practice reinforces training and education and helps achieve the greatest benefit from the time and resources expended. Exercises provide this kind of practice in a practical way that includes discussing or simulating the unwanted kinds of events that may involve critical infrastructure. There are many different types of exercises, including: discussion-based workshops or seminars; facilitated discussions with multiple agencies and infrastructure operators about a specific scenario (known as a tabletop exercise); drills of specific plans or activities; simulated events (functional exercises); and actual responses to artificial events (known as full-scale exercises).

An additional benefit of training and education efforts is building relationships among the stakeholders, particularly in practical exercises. Developing greater trust and understanding within a sector facilitates a more effective response in times of crisis.

Creating a culture of continuous improvement in infrastructure security and resilience also requires increasing the exposure to fundamental concepts in certain college or university curricula as well. The purpose of academic programs may be to: train students on the use of assessment techniques; make engineers more aware of ways to protect infrastructure elements, reduce their vulnerabilities, or make them more resilient by design; inform planners on the importance of advance planning, information sharing, and partnerships; help emergency managers understand the potential impacts of cascading failures; among other factors.

Potential Training Topics

- Best practices for physical security
- Active Shooter
- Identifying and Reporting Suspicious Activity
- Insider Threat
- Credentialing
- Bag Screening
- Patron Screening
- Sector Best Practices (e.g., chemical, energy, water)
- Supply chain risk management and third party dependency
- Incident Management and Response
- Bomb Threats
- Countering Improvised Explosive Devices
- Vehicle Threats
- Suicide Bombers
- Cybersecurity
- Exercises
- Terrorism Threats, Tactics, and Trends
- ICS and Operational Technology
- Risk Assessment (Threat, Vulnerability, and/or Consequence) and Mitigation

Selected Resources

1. Critical Infrastructure Training webpage has links to many different training offerings; others are provided by professional societies, individual companies, trade associations, and academic institutions. (https://www.dhs.gov/critical-infrastructure-training)
2. An example of an exercise for the electric grid (http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx)
3. The Communications-Specific Tabletop Exercise Methodology provides an example that can be refined and further developed to exercise and evaluate specific areas of concern for communications infrastructure owners and operators. (https://www.dhs.gov/sites/default/files/publications/CommunicationsSpecificTabletopExerciseMethodology.pdf)
4. CISA Hometown Security. (https://www.cisa.gov/hometown-security)

Evaluating the Program

Once you have set up a program to assess and address threats to critical infrastructure, it is a good practice to periodically evaluate that program. A key challenge in evaluation is measuring critical infrastructure security and resilience programs because of the breadth and diversity of a program's infrastructure—across numerous sectors, levels of government, and types of owners and operators.

There are two competing imperatives:

- Designing common and consistent measurements to compare performance across sectors, activities, and regions and to prioritize gaps; and
- Customizing performance measurements that fit the unique needs of each reporting situation.

Metrics or performance measures should be simple and repeatable, and should be used to establish accountability; document actual performance; facilitate identification of shortcomings or gaps; identify corrective actions; increase the effectiveness of risk management; and help reassess goals, objectives, and timelines.

A hybrid of metrics common to all industry sectors and those metrics tailored to each element within a sector may help address the competing imperatives. Performance measures should address process-based outputs (such as numbers of assessments or activities) and outcomes (such as reductions in risk or improvements in resilience) and should evaluate progress towards goals and objectives. Routine reporting of performance should be outlined to document the critical infrastructure security and resilience program, as well as to determine appropriate adjustments.

Similarly, data collection processes, systems, and tools as well as analytic approaches must be identified. This can be difficult if the overall critical infrastructure security and resilience program is voluntary and data is considered proprietary by the infrastructure owners and operators. It may be helpful to coordinate with overseeing government agencies, particularly those that already collect information on the operational performance of specific sectors as they may have resolved some of the collection barriers, at least at a high level.

Value Proposition/Business Case

- Measuring performance succinctly articulates the value proposition or business case. What can companies or governments expect to obtain as a result of their engagement in the process?
- Do they learn more about best practices that can make them more competitive? Is their liability reduced in some way? Are there benefits that some of the mitigation measures offer to daily operations? Can local governments better plan the expenditure of their resources? Are they contributing measurably to the security and resilience of their company and/or the country?
- Capturing successes resulting from the program and promoting them will help establish the value proposition or business case.

Selected Resources

1. Emergency Services Sector – Continuity Planning Suite. (https://www.cisa.gov/emergency-services-sector-continuity-planning-suite)
2. Cybersecurity Assessments. (https://www.cisa.gov/cybersecurity-assessments).
3. National Infrastructure Advisory Council Evaluation and Enhancement of Information Sharing and Analysis: Final Report and Recommendations. (https://www.cisa.gov/publication/niac-eval-enhance-info-sharing-final-report).

Promoting the Program

Critical infrastructure security and resilience impacts everyone. While not all stakeholders are engaged in the more detailed elements of the program, they still need a high-level understanding of the risks so they have adequate information and greater confidence in their decisions regarding risk mitigation and management activities — especially those that may require changes in their daily operations and lives.

Stakeholders may include individual companies, the general public, local governments, and many others. To reach these diverse audiences, marketing campaigns such as the "See Something, Say Something" effort in the United States may be useful. This effort has successfully reached beyond infrastructure partners to involve the whole community and increase their situational awareness. Other outreach and awareness efforts may draw on existing communications channels used by industry associations and trade groups.

The messages for different audiences should center on certain key messages that capture – in clear and simple language –the issue at hand, how it affects their interest, and the essence of the desired actions for each of the target audiences. What should the public regard as suspicious activities, and how should they report them? Who should companies contact for more information about security and resilience measures and best practices in their specific industries? How can local or regional governments become more involved?

The different audiences should be identified so that the available resources for outreach and awareness are used efficiently, and reflect the role of each audience in improving infrastructure security and resilience.

Communication Channels

- Web pages
- Social media
- Web-enabled training
- Public media
- Executive briefings
- Technical presentations and exhibits at conferences
- Seminars tailored to different audiences
- Trade publications
- Electronic news organizations
- Press releases
- Special events

Selected Resources

1. Representative outreach and awareness material can be found at: Hometown Security web page (https://www.cisa.gov/hometown-security)
2. Active Shooter Preparedness web page (https://www.cisa.gov/active-shooter-preparedness)
3. Office for Bombing Prevention web page (https://www.cisa.gov/office-bombing-prevention-obp)
4. If You See Something, Say Something web page (https://www.dhs.gov/see-something-say-something)

Conclusion

Critical infrastructure is the foundation on which daily vital societal and economic functions depend, and disruption or loss to any element of critical infrastructure has the potential to severely impact our lives. Working together and sharing good practices, approaches, and experiences will help promote and enhance national – and global – critical infrastructure security and resilience today and in the future.

CISA
CYBER+INFRASTRUCTURE