# Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach

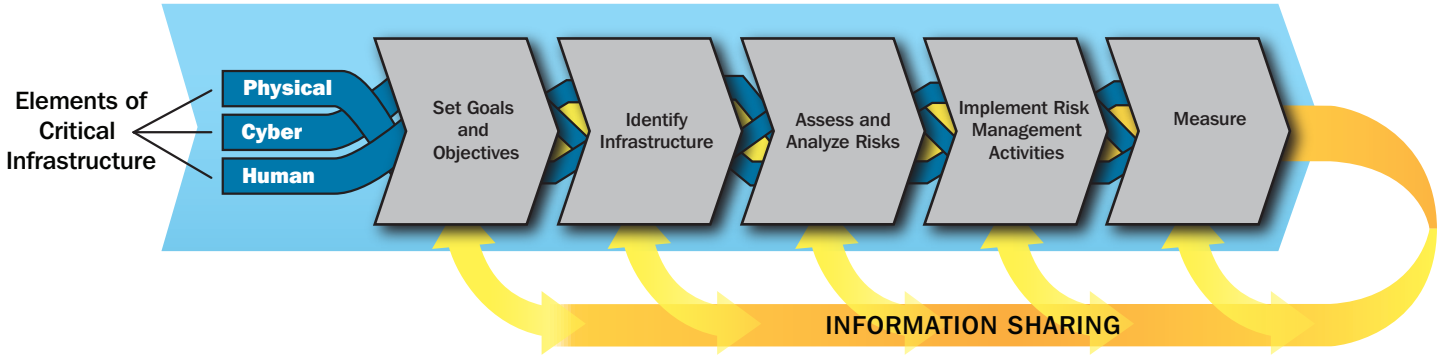
Homeland Security

# Executing a Critical Infrastructure Risk Management Approach

Risk is defined as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences[1]. It is influenced by the nature and magnitude of a threat or hazard, the vulnerabilities from that threat or hazard, and the consequences that could result. Risk information allows partners, from facility owners and operators to Federal agencies, to prioritize risk management efforts.

This supplement describes a useful critical infrastructure risk management approach, which supports the risk management framework depicted in Figure 1. The framework enables the integration of strategies, capabilities, and governance structures to enable risk-informed decision making related to the Nation's critical infrastructure. The critical infrastructure risk management approach described in this supplement can be applied to all threats and hazards, including cyber incidents, natural disasters, man-made safety hazards, and acts of terrorism, although different information and methodologies may be used to understand each.

**Figure 1: Critical Infrastructure Risk Management Framework**




In addition, the critical infrastructure risk management approach complements and supports the Threat and Hazard Identification and Risk Assessment (THIRA) process conducted by regional, State, and urban area jurisdictions. The THIRA process involves identifying threats and hazards and how they may affect a community and determining how best to mitigate those threats and hazards, based on current capabilities and resource requirements. This process aligns with steps in the critical infrastructure risk management framework, as described in applicable sections of this supplement. The THIRA process is supported by a Strategic National Risk Assessment (SNRA) that analyzes the greatest risks facing the Nation. Taken together, individual THIRAs, the SNRA, and more specialized risk assessments (such as

[1] U.S. Department of Homeland Security, DHS Risk Lexicon, 2010.

sector-specific and other critical infrastructure risk assessments), provide an integrated national risk picture, which helps to achieve the National Preparedness Goal of a more secure and resilient Nation.

Many government and industry partners use other risk management models, which can be more detailed and often are tailored to a specific need. The critical infrastructure risk management framework is not intended to replace any such models or processes already in use. Rather, it supports a common, unifying approach to risk management that all critical infrastructure partners can use, relate to, and align with their own risk management models and activities.

The critical infrastructure risk management approach can be tailored toward and applied on an asset, system, network, or functional basis, depending on the fundamental characteristics of the decisions it is intended to support and the nature of the related infrastructure. Those sectors and entities primarily dependent on fixed assets and physical facilities may find a bottom-up, asset-by-asset approach to be most appropriate. Sectors such as Communications, Information Technology, and Food and Agriculture, with accessible and distributed systems, may find a top-down, business or mission continuity approach that uses risk assessments focused on network and system interdependencies to be more effective.

The critical infrastructure risk management approach described below includes the following activities:

- **Set Goals and Objectives:** Define specific outcomes, conditions, end points, or performance targets that collectively describe an effective and desired risk management posture.
- **Identify Infrastructure:** Identify assets, systems, and networks that contribute to critical functionality and collect information pertinent to risk management, including analysis of dependencies and interdependencies.
- **Assess and Analyze Risks:** Evaluate the risk, taking into consideration the potential direct and indirect consequences of an incident, known vulnerabilities to various potential threats or hazards, and general or specific threat information.
- **Implement Risk Management Activities:** Make decisions and implement risk management approaches to control, accept, transfer, or avoid risks. Approaches can include prevention, protection, mitigation, response, and recovery activities.
- **Measure Effectiveness:** Use metrics and other evaluation procedures to measure progress and assess the effectiveness of efforts to secure and strengthen the resilience of critical infrastructure.

This approach supports an integrated and continuing process with feedback loops and iterative steps. It enables a critical infrastructure decision maker to track progress and implement actions to improve critical infrastructure security and resilience over time. The physical, cyber, and human elements of critical infrastructure should be considered as part of each aspect of the risk management approach.

# 1. Set Goals and Objectives

Goals and objectives are likely to vary across sectors and organizations, depending on the risk landscape, operating environment, and composition of a specific industry, resource, or other aspect of critical infrastructure. Nationally, the overall goal of critical infrastructure risk management is an enhanced state of security and resilience achieved through the implementation of focused risk management activities within and across sectors and levels of government.

The *National Plan* sets forth the following goals for the national effort to strengthen critical infrastructure security and resilience:

- 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, 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; and
- Promote learning and adaptation during and after exercises and incidents.

The critical infrastructure risk management approach supports these goals by:

- Enabling the development of national, State, regional, and sector risk profiles that support the National Critical Infrastructure Security and Resilience Annual Report. These risk profiles outline the highest risks facing different sectors and geographic regions and identify cross-sector or regional issues of concern that are appropriate for the Federal critical infrastructure focus, as well as opportunities for sector, State, and regional initiatives.
- Enabling the critical infrastructure community to determine the best courses of action to reduce potential consequences, threats, and/or vulnerabilities, and, in turn, reduce risk. Some available options include encouraging voluntary implementation of focused risk management strategies (e.g., through public-private partnerships), applying standards and best practices, pursuing economic incentive-related policies and programs, and conducting additional information sharing, if appropriate.
- Informing the identification of risk management and resource allocation options, rather than specifying requirements for critical infrastructure owners and operators.

From a sector or jurisdictional perspective, critical infrastructure security and resilience goals and their supporting objectives should:

- Consider distinct assets, systems, networks, functions, operational processes, business environments, and risk management approaches;
- Define the risk management posture that critical infrastructure partners seek to attain individually or collectively; and
- Express this posture in terms of the objectives and outcomes sought.

Taken together, these goals and objectives guide all levels of government and the private sector in tailoring risk management programs and activities to address critical infrastructure security and resilience needs.

# 2. Identify Infrastructure

Critical infrastructure partners view criticality differently, based on their unique situations, operating models, and associated risks. Partners—both public and private—identify the infrastructure that they consider essential to their operations and efforts for improving and enhancing security and resilience. The Federal Government works with partners to determine which assets, systems, and networks are nationally significant and identify those that are essential to their continued operations. Some sectors identify regional, State, and locally significant infrastructure as a joint activity between government and industry partners. Private sector owners and operators may identify additional infrastructure that are necessary to keep their businesses running to provide goods and services to their customers. Similarly, State, local, tribal, and territorial (SLTT) governments may identify those assets, systems, and networks that are crucial to their continued operations to ensure public health and safety and the provision of essential services.

The Department of Homeland Security's National Critical Infrastructure Prioritization Program (NCIPP) identifies nationally significant infrastructure to support risk-informed decision making by the Federal Government and its critical infrastructure partners. Critical assets, systems, and networks identified through this process include those which, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, or widespread and long-term impacts to national well-being and governance capacity. The NCIPP identifies, collects, and prioritizes critical infrastructure information from States, critical infrastructure sectors, and other homeland security partners across the Nation. It uses an enhanced infrastructure data collection application, which provides the ability to input data throughout the year.

Data collected through the NCIPP form the basis of a national inventory that includes those assets, systems, and networks that are nationally significant and those that may not be significant on a national level but are, nonetheless, important to State, local, or regional critical infrastructure security and resilience and national preparedness efforts. The national inventory includes relevant information for natural disasters, industrial accidents, and other incidents. Critical infrastructure partners work together to ensure that the inventory data structure is accurate, current, and secure.

Federal Government partners, including the Sector-Specific Agencies (SSAs), work with critical infrastructure owners and operators and SLTT entities to build upon and update existing inventories at the State and local levels that are regionally and locally significant.

## Cyber Infrastructure

The *National Plan* addresses security and resilience of the cyber elements of critical infrastructure in an integrated manner rather than as a separate consideration. During the risk assessment process, cyber system components should be identified individually or be included as a cyber element of a larger asset, system, or network with which they are associated. The identification process should include information on international cyber infrastructure with cross-border implications, interdependencies, or cross-sector ramifications.

Cyber system elements that exist in most, if not all, sectors include business systems, control systems, access control systems, and warning and alert systems. The Internet has been identified as a key resource, comprising the domestic and international assets within both the Information Technology and Communications Sectors; the need for access to and reliance on information and communications technology is common to all sectors.

DHS helps SSAs and other critical infrastructure partners identify cyber assets, systems, and networks, including those involving multiple sectors. Several sectors have developed a functions-based approach for identifying cyber-dependent critical infrastructure. The Cyber-Dependent Infrastructure Identification[2] approach is based on three high-level steps, which include:

- Defining criteria for "catastrophic" impacts across all sectors;
- Evaluating previous sector efforts to determine how they can be leveraged to identify cyber-dependent critical infrastructure at greatest risk; and
- Applying a functions-based approach to identify cyber-dependent infrastructure and its impacts on the sector.

[2] Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013.

In addition, DHS, in collaboration with other critical infrastructure partners, provides cross-sector cyber methodologies, which enable sectors to identify cyber assets, systems, and networks that may have nationally significant consequences if destroyed, incapacitated, or exploited. These methodologies also characterize the reliance of a sector's business and operational functionality on cyber systems.

# 3. Assess and Analyze Risks

Homeland security risks can be assessed in terms of their likelihood and potential consequences. Common definitions, scenarios, assumptions, metrics, and processes can ensure that risk assessments contribute to a shared understanding among critical infrastructure partners. The risk management approach supports an assessment strategy that results in sound, scenario-based consequence and vulnerability estimates, as well as an assessment of the likelihood that the postulated threat or hazard will occur.

As stated in the introduction to this supplement, it is important to think of risk as influenced by the nature and magnitude of a threat or hazard, the vulnerabilities to that threat or hazard, and the consequences that could result.

- **Threat:** A natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. For the purpose of calculating risk, the threat of an unintentional hazard is generally estimated as the likelihood that a hazard will manifest itself. Intentional hazard is generally estimated as the likelihood of an attack being attempted by an adversary. In the case of intentionally adversarial actors and actions, for both physical and cyber effects, the threat likelihood is estimated based on the intent and capability of the adversary.
- **Vulnerability:** A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given threat or hazard. In calculating the risk of an intentional threat, a common measure of vulnerability is the likelihood that an attack is successful, given that it is attempted.
- **Consequence:** The effect of an event, incident, or occurrence. It reflects the level, duration, and nature of the loss resulting from the incident. Potential consequences may include public health and safety (i.e., loss of life and illness), economic (direct and indirect), psychological, and governance/mission impacts.

Critical infrastructure risk assessments can explicitly consider each of these factors, but do not have to do so in a quantifiable manner. In conducting assessments, analysts should be very careful when calculating risk to properly address interdependencies and any links between how the threats and vulnerabilities were calculated to ensure that the results are sound and defensible.

## Critical Infrastructure Risk Assessments

Risk assessments are conducted by many critical infrastructure partners to meet their own decision-making needs, using a broad range of methodologies. As a general rule, simple but defensible methodologies are preferred over more complicated methods. Simple methodologies are more likely to fulfill the requirements of transparency and practicality.

Risk methodologies are often grouped into qualitative and quantitative categories, but when well-designed, both types of assessments have the potential to deliver useful analytic results. Similarly, both qualitative and quantitative methodologies can be needlessly complex or poorly designed. The methodology that best meets the decision maker's needs is generally the best choice, whether quantitative or qualitative.

The common analytic principles originally provided in the *National Infrastructure Protection Plan* are broadly applicable to all parts of a risk methodology. These principles provide a guide for improving existing methodologies or modifying them so that the investment and expertise they represent can be used to support national-level, comparative risk assessments, investments, incident response planning, and resource prioritization. Recognizing that many risk assessment methodologies are under development and others evolve in a dynamic environment, the analytic principles for risk assessment methodologies serve as a guide to future adaptations. The basic analytic principles ensure that risk assessments are:

- **Documented:** The methodology and the assessment must clearly document what information is used and how it is synthesized to generate a risk estimate. Any assumptions, weighting factors, and subjective judgments need to be transparent to the user of the methodology, its audience, and others who are expected to use the results. The types of decisions that the risk assessment is designed to support and the timeframe of the assessment (e.g., current conditions versus future operations) should be given.
- **Reproducible:** The methodology must produce comparable, repeatable results, even though assessments of different critical infrastructure may be performed by different analysts or teams of analysts. It must minimize the number and impact of subjective judgments, leaving policy and value judgments to be applied by decision makers.
- **Defensible:** The risk methodology must logically integrate its components, making appropriate use of the professional disciplines relevant to the analysis, as well as be free from significant errors or omissions. Uncertainty associated with consequence estimates and confidence in the vulnerability and threat estimates should be communicated.

## Risk Scenario Identification

Homeland security risk assessments generally should use scenarios to divide the identified risks into separate pieces that can be assessed and analyzed individually. A scenario is a hypothetical situation consisting of an identified threat or hazard, an entity impacted by that hazard, and associated conditions including consequences, when appropriate.

When analysts are developing plausible scenarios to identify potential risks for an assessment, the set of scenarios should cover the full scope of the assessment and provide the decision maker with complete information. For a relatively fixed system, it is important to identify those components or critical nodes where potential consequences would be highest and where security and resilience activities can be focused. Analysts should take care when dealing with the results; including multiple scenarios that contain the same event could lead to double counting the risk.

## Threat and Hazard Assessment

The Federal Government assesses the current terrorist threat to the United States through extensive study and understanding of terrorists and terrorist organizations, and frequently depends on analysis of classified information. It provides its partners with unclassified assessments of potential terrorist threats and appropriate access to classified assessments where necessary and authorized. These threat assessments are derived from analyses of adversary intent and capability, and describe what is known about terrorist interest in particular critical infrastructure sectors, as well as specific attack methods. Since international terrorists, in particular, have continually demonstrated flexibility and unpredictability, the Federal Government also analyzes known terrorist goals, objectives, and developing capabilities to provide critical infrastructure owners and operators with a broad view of the potential threat and postulated terrorist attack methods. Similar approaches are used to assess the threats of theft, vandalism, sabotage, insider threat, cyber threats, active shooter, and other deliberate acts.

Both domestic and international critical infrastructure assets represent potential prime targets for adversaries. Given the deeply rooted nature of these goals and motivations, critical infrastructure likely will remain highly attractive targets for state and non-state actors and others with ill intent. Threat assessments must address the various elements of both physical and cyber threats to critical infrastructure, depending on the attack type and target.

Hazard assessments draw on historical information and future predictions about natural hazards to assess the likelihood or frequency of various hazards. This is an area where various components of the Federal Government work with sector leadership and owners and operators to make assessments in advance of any specific hazard as well as once an impending hazard (such as a hurricane yet to make landfall) is identified. Hazard assessments increasingly consider factors such as the impacts of aging

infrastructure and climate change on overall security and resilience. Threats and hazards to the critical infrastructure within a community are included among the threats and hazards identified through the THIRA process.

## Vulnerability Assessment

Vulnerabilities may be associated with physical (e.g., no barriers or alarm systems), cyber (e.g., lack of a firewall), or human (e.g., untrained guards) factors. A vulnerability assessment can be a stand-alone process or part of a full risk assessment and involves the evaluation of specific threats to the asset, system, or network under review to identify areas of weakness that could result in consequences of concern.

Many Sector-Specific Plans (SSPs) describe different vulnerability assessment methodologies used in specific critical infrastructure sectors. The SSPs also may provide specific details regarding different ways the assessments can be carried out (e.g., by whom and how often).

## Consequence Assessment

Consequence categories may include:

- **Public Health and Safety:** Effect on human life and physical well-being (e.g., fatalities, injuries/illness).
- **Economic:** Direct and indirect economic losses (e.g., cost to rebuild asset, cost to respond to and recover from attack, downstream costs resulting from disruption of product or service, long-term costs due to environmental damage).
- **Psychological:** Effect on public morale and confidence in national economic and political institutions. This encompasses those changes in perceptions emerging after a significant incident that affect the public's sense of safety and well-being and can manifest in aberrant behavior.
- **Governance/Mission Impact:** Effect on the ability of government or industry to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

Consequence analysis ideally should address both direct and indirect effects. Many assets, systems, and networks depend on connections to other critical infrastructure to function. For example, nearly all sectors rely on the essential functions of energy, communications, transportation, and water. In many cases, the failure of one asset or system will affect the ability of interrelated assets or systems in the same or another sector to perform necessary functions. Furthermore, cyber interdependencies present unique challenges for all sectors because of the borderless nature of cyberspace. Interdependencies are dual in nature. For example, the Energy Sector relies on computer-based control systems to manage the electric power grid, while those same control systems require electric power to operate. As a result,

complete consequence analysis addresses multidirectional critical infrastructure interconnections for the purposes of risk assessment.

The level of detail and specificity achieved by using the most sophisticated risk assessment models and simulations may not be practical or necessary for all assets, systems, or networks. In these circumstances, a simplified dependency and interdependency analysis based on expert judgment may provide sufficient insight to make informed risk management decisions in a timely manner.

There is also an element of uncertainty in consequence estimates. Even when a scenario with reasonable worst-case conditions is clearly stated and consistently applied, there is a range of outcomes that could occur. For some incidents, the consequence range is small, and a simple estimate may provide sufficient information to support decisions. If the range of outcomes is large, the scenario may require more specificity about conditions to obtain appropriate estimates of the outcomes. However, if the scenario is broken down to a reasonable level of granularity and there is still significant uncertainty, the estimate should be accompanied by the uncertainty range to support more informed decision making. The best way to communicate uncertainty will depend on the factors that make the outcome uncertain, as well as the amount and type of information that is available.

# 4. Implement Risk Management Activities

The results of critical infrastructure risk assessments inform the selection and implementation of mitigation activities and the establishment of risk management priorities for critical infrastructure owners and operators. Similarly, the results of THIRAs, which may include critical infrastructure risk assessments, can inform the selection of risk management options and core capability priorities for entire communities. The selection and implementation of appropriate risk management activities helps to focus planning, increase coordination, and support effective resource allocation and incident management decisions. Comparing and prioritizing the risks faced by different entities helps identify where risk mitigation is most needed and determines and helps justify the selection of the most cost-effective risk management options. This supports resource allocation decisions (such as where risk management programs should be instituted), guides investments in these programs, and highlights the measures that offer the greatest return on investment.

The process of evaluating and selecting effective risk management activities generates information that can be used during incident response to help inform decisions regarding critical infrastructure restoration. It also provides the basis for understanding potential risk mitigation benefits that are used to inform planning and resource decisions.

Critical infrastructure partners rely on different approaches for selecting risk management activities, according to their specific authorities, sector needs, risk landscapes, security approaches, and business

environment. For example, owners and operators, Federal agencies, and State and local authorities all have different options available to them to help reduce risk. Asset-focused priorities may be appropriate for critical infrastructure with risks predominantly associated with facilities, the local environment, and physical attacks, especially those that can be exploited and used as weapons. Function-focused priorities may be more effective at ensuring continuity of operations during and after an incident in sectors where critical infrastructure resilience may be more important than physical protection and critical infrastructure hardening. Programs intended to reduce critical infrastructure risk will prioritize investments that secure physical assets or ensure resilience in virtual systems, depending on which option best enables cost-effective critical infrastructure risk management.

Critical infrastructure owners and operators prioritize and implement risk mitigation activities based on their cost-effectiveness, feasibility, and potential for risk reduction. In assessing risks and evaluating options for managing them, both the THIRA process and the critical infrastructure risk management approach help to identify capability gaps and determine capabilities that need to be developed or enhanced.

Risk management actions include measures designed to deter, disrupt, and prepare for threats and hazards; reduce vulnerability to an attack or other disaster; mitigate consequences; and enable timely, efficient response and restoration in a post-event situation, whether a terrorist attack, natural disaster, or other incident. The risk management approach focuses attention on those prevention, protection, mitigation, response, and recovery activities that bring the greatest return on investment, not simply the vulnerability reduction to be achieved. Security and resilience activities vary between sectors and jurisdictions and across a wide spectrum of actions designed to secure and strengthen the resilience of critical infrastructure.

Risk management activities also may include the means for reducing the consequences of an attack or incident. These actions are focused on mitigation, response, and/or recovery. Often it is more cost-effective to build security and resilience into assets, systems, and networks than to retrofit them after initial development and deployment. Accordingly, critical infrastructure partners should consider how risk management, robustness, and appropriate physical and cyber security enhancements can be incorporated into the design and construction of new critical infrastructure and the redesign or repair of existing infrastructure. In situations where robustness and resilience are key to managing critical infrastructure risk, it may be more effective and efficient to implement programs at the system level rather than at the individual asset level. For example, it may not be cost-effective to make every hospital in a metropolitan area resilient but it would be prudent to make sure that geographically or otherwise affiliated hospitals are robust as a group or system, so that one can step in for another in the event of a disaster.

When evaluating risk management options, organizations should consider industry standards and best practices, measures applied effectively in other settings, and lessons learned from actual events and exercises. Risk management options should be described in enough detail to define the extent to which they will reduce the elements of risk and the life-cycle costs of each option should be estimated (e.g., initial investment or startup, operation and maintenance, and, for physical options, demolition and disposal when their usefulness has ended). It is important to review the candidate options for synergies (e.g., instances where risk reduction options designed for one scenario affect the risk—positively or negatively—of other scenarios). Exploiting positive synergies and avoiding negative ones allows entities to select cost-effective options to reduce risk.

Effective risk management activities are comprehensive, coordinated, and cost-effective. Risk management decisions should be made based on an analysis of the costs and other impacts, as well as the projected benefits of identified courses of action—including the no-action alternative if a risk is considered to be effectively managed already. It is important to note that risk management actions can be evaluated based on their potential to manage risk in the aggregate across a range of scenarios, as well as their ability to manage risks associated with a single scenario; maintaining both perspectives is crucial in identifying the most effective actions.

# 5. Measure Effectiveness

The use of performance metrics is an important step in the critical infrastructure risk management process to enable assessment of improvements in critical infrastructure security and resilience. Performance metrics allow partners to track progress against priorities and against their goals and objectives. The metrics provide a basis for the critical infrastructure community to establish accountability, document actual performance, promote effective management, and provide a feedback mechanism to inform decision making.

The national goals, which focus on risk management, shared situational awareness, and national preparedness, will be central to effectively assessing progress, providing a common understanding of the desired "end state" the voluntary partnership is collectively working to achieve. Developed through a participatory process involving a wide range of critical infrastructure partners, a complementary set of national priorities will illustrate the broad courses of action necessary to achieve the national goals.

The critical infrastructure community will develop high-level outputs or outcomes associated with the national goals and priorities, to facilitate measurement of progress toward the ultimate outcome of critical infrastructure security and resilience established in PPD-21.

With this common understanding as a baseline, the critical infrastructure community can demonstrate progress toward the national goals using available data and information. When significant progress has been made toward the national-level goals and priorities—or as the risk environment, policy landscape, and field of practice evolve—the community will review and update these goals and priorities. Sectors and regional partnerships should develop goals complementary to the national goals but tailored to the specific sector or geographic area.

## Using Metrics and Performance Measurement for Continuous Improvement

By using metrics to evaluate the effectiveness of voluntary partnership efforts to achieve national and sector priorities, critical infrastructure partners can adjust and adapt their security and resilience approaches to account for progress achieved, as well as changes in the threat and other relevant environments. Metrics are used to focus attention on areas of security and resilience that warrant additional resources or other changes through an analysis of challenges and priorities at the national, sector, and owner/operator levels.

Metrics also serve as a feedback mechanism for other aspects of the critical infrastructure risk management approach. They can inform progress against national and sector goals and provide analysts with information to adjust their risk assessments. For instance, metrics indicate the effectiveness of security and resilience activities and the extent to which these activities are reducing risks. Finally, metrics can inform the process of prioritizing and selecting the most effective and cost-efficient ways to manage risk.


Homeland
Security