

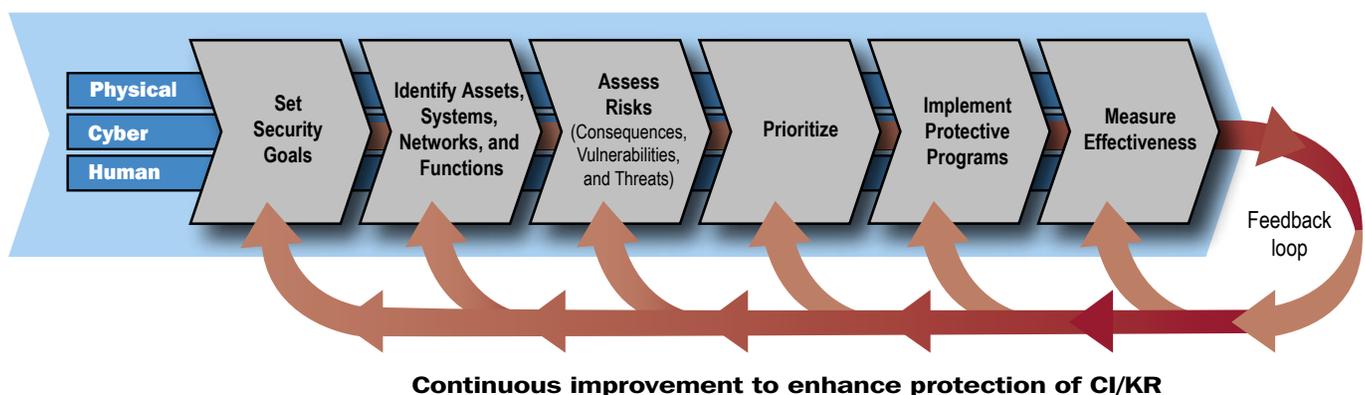
3. The Protection Program Strategy: Managing Risk

The cornerstone of the NIPP is its risk management framework. Risk is generally defined as the combination of the frequency of occurrence, vulnerability, and the consequence of a specified hazardous event. In the context of the NIPP, risk is the expected magnitude of loss (e.g., deaths, injuries, economic damage, loss of public confidence, or government capability) due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss. The NIPP risk management framework (see figure 3-1) establishes the process for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector-specific risk that drives CI/KR protection activities. The framework applies to the general threat environment, as well as to specific threats or incident situations. In the case of natural disasters and accidents, the incident management community has access to risk assessment tools such as the models used by the National Hurricane Center (NHC) and the fault trees used by the NRC. Because similar models are not yet in broad use for terrorist threats, the NIPP provides an augmented framework for the terrorist-related aspects of threat analysis.

This chapter addresses the use of the risk management framework as part of the overall effort to ensure a steady-state of protection within and across the CI/KR sectors. DHS, the SSAs, and their security partners share responsibility for implementation of the NIPP risk management framework. SSAs are responsible for leading sector-specific risk management programs and for ensuring that the tailored, sector-specific application of the risk management framework is addressed in their respective SSPs. DHS supports these efforts by providing guidance, tools, and analytical support to SSAs

and other security partners. DHS, in collaboration with other security partners, is responsible for using the results obtained in sector-specific efforts to conduct cross-sector risk analysis and management activities. This includes the assessment of dependencies, interdependencies, and cascading effects; identification of common vulnerabilities; development and sharing of common threat scenarios; development and sharing of cross-sector measures to reduce or manage risk; and identification of specific R&D needs.

Figure 3-1: NIPP Risk Management Framework



The risk management framework is tailored and applied on an asset, system, network, or function basis, depending on the fundamental characteristics of the individual CI/KR sectors. For those sectors primarily dependent on fixed assets and physical facilities, a bottom-up, asset-by-asset approach may be most appropriate. For sectors with diverse and logical assets, such as Telecommunications and Information Technology, a top-down, business or mission continuity approach that focuses on networks, systems, and functions may be more effective. Each sector chooses the approach that produces the most actionable results for the sector and works with DHS to ensure that the relevant risk analysis procedures are compatible with the criteria established in the NIPP.

The NIPP risk management framework includes the following activities:

- **Set security goals:** Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.
- **Identify assets, systems, networks, and functions:** Develop an inventory of the assets, systems, and networks, including those located outside the United States, that comprise the Nation's CI/KR and the critical functionality therein; collect information pertinent to risk management that takes into account the fundamental characteristics of each sector.
- **Assess risks:** Determine risk by combining potential direct and indirect consequences of a terrorist attack or other hazards (including seasonal changes in consequences, and dependencies and interdependencies associated with each identified asset, system, or network), known vulnerabilities to various potential attack vectors, and general or specific threat information.
- **Prioritize:** Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk; establish priorities based on risk; and determine protection and business continuity initiatives that provide the greatest mitigation of risk.
- **Implement protective programs:** Select sector-appropriate protective actions or programs to reduce or manage the risk identified; secure the resources needed to address priorities.
- **Measure effectiveness:** Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national CI/KR protection program in improving protection, managing risk, and increasing resiliency.

The NIPP is based on the principle of risk management, combining consequence, vulnerability, and threat information. Whether a top-down or bottom-up approach is used, the goal is the same: identify those key assets, systems, networks, and functions most in need of focused risk mitigation measures.

DHS and the SSAs use information from metrics and other evaluation tools to support continuous improvement. Information about the current status of each sector is compared to the baseline of information collected and analyzed during initial risk assessments to measure progress over time. This process forms a feedback loop, which allows the Federal Government and its security partners to track progress and implement actions to improve national CI/KR protection and resiliency.

The physical, cyber, and human elements of CI/KR are considered during each step of the risk management framework. The sector partnership model discussed in chapter 4 provides the structure for coordination and management of risk management activities that are tailored to each sector.

3.1 Set Security Goals

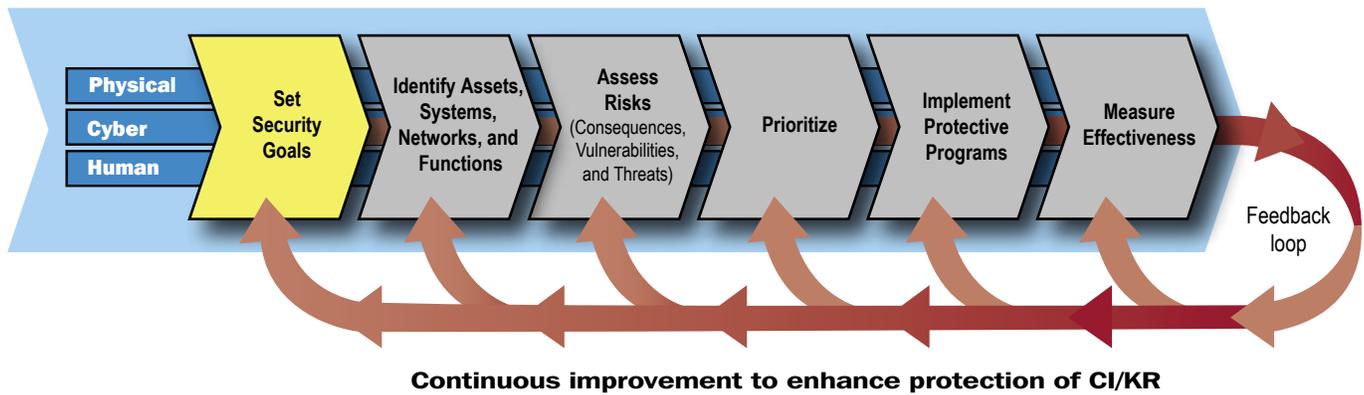
Achieving a robust, protected, and resilient infrastructure requires national and sector-specific homeland security goals that collectively represent the desired security posture. These goals should consider the physical, cyber, and human elements of CI/KR protection. Security goals may vary across and within sectors, depending on the internal structure and composition of a specific industry, resource, or other aspect of CI/KR.

Nationally, the overall goal of risk management efforts is an enhanced state of CI/KR protection achieved through the implementation of focused risk-mitigation and protective strategies within and across sectors. The risk management framework supports this goal by:

Sample Security Goal Telecommunications Sector

Build networks and systems that provide secure and resilient communications for the Nation and that can be rapidly restored after a natural or manmade disaster.

Figure 3-2: NIPP Risk Management Framework: Set Security Goals



- Supporting the development of the national risk profile presented in the National CI/KR Protection Annual Report described in chapter 7. This is a high-level summary of the aggregate risk and the protective status of all sectors. It is developed by DHS in collaboration with other security partners, updated on an ongoing basis, and used to support strategic decisionmaking, planning, and resource allocation;
- Enabling DHS, SSAs, and other security partners to determine the best courses of action to reduce potential consequences, threats, or vulnerabilities. Some available options include encouraging voluntary implementation of focused risk management strategies (e.g., through public-private partnerships), pursuing economic incentive-related policies and programs, and undertaking regulatory action if appropriate; and
- Using prioritized information to identify, or create, specific protective programs for CI/KR of the highest criticality based on risk. Depending on the protective program, resource allocation may occur at the Federal, State, Territorial, local, or tribal level, or may be solely the responsibility of CI/KR owners and operators. International outreach and collaboration also may be required in many circumstances.

From a sector perspective, security goals or their related supporting objectives:

- Define the protective (and, if appropriate, the response or recovery) posture that security partners seek to attain;
- Express this posture in terms of objective metrics and the time required to attain it through specific supporting objectives;

- Consider distinct assets, systems, networks, operational processes, business environments, and risk management approaches; and
- Vary according to the specific business characteristics and security landscape of the affected sector, jurisdiction, or locality.

Taken collectively, these goals guide all levels of government and the private sector in tailoring protective programs and activities to address CI/KR protection needs.

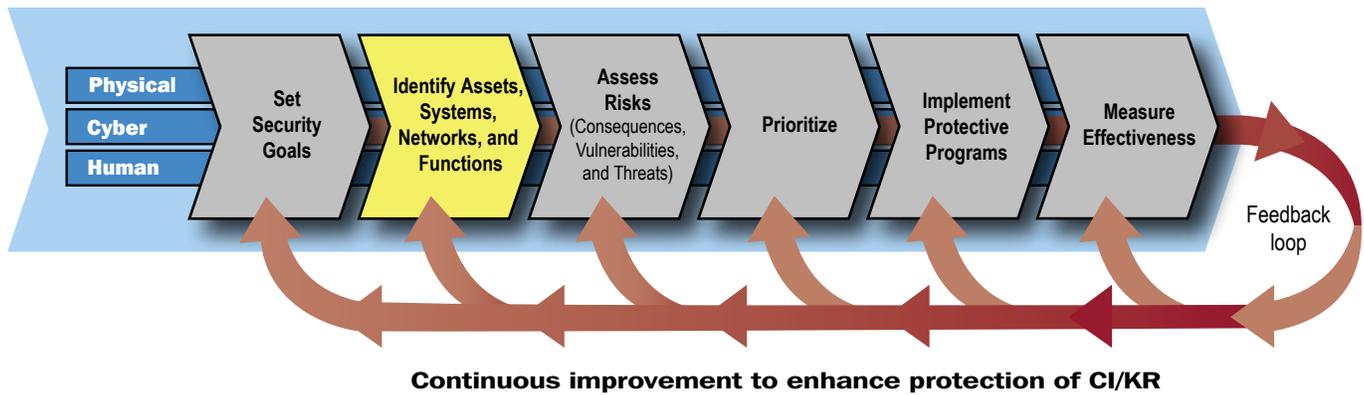
3.2 Identify Assets, Systems, Networks, and Functions

To meet its responsibilities under the Homeland Security Act and HSPD-7, DHS maintains a comprehensive national inventory of the information needed to identify those assets, systems, networks, and functions that make up the Nation's CI/KR. This information may be different for each sector because it is collected on an asset, system, network, or function basis, as determined by the fundamental characteristics of each sector.

3.2.1 National Infrastructure Inventory

The inventory addresses the physical, cyber, and human elements of each asset, system, network, or function under consideration. The compilation process relies on the substantial body of previous assessments that have been completed for natural disasters, industrial accidents, and other incidents. The inventory includes basic information on the relationships, dependencies, and interdependencies between various assets, systems, networks, and functions; on service providers, such as schools and businesses, that may be of relevance

Figure 3-3: NIPP Risk Management Framework: Identify Assets, Systems, Networks, and Functions



to more than one sector; and on the foreign assets, systems, networks, and functions on which U.S. CI/KR may rely. The inventory also includes a cyber data framework that is used to characterize each sector’s unique cyber assets, systems, networks, or functions.

DHS compiles the inventory in a manner that enables it to be quickly scanned, searched, and analyzed. This allows DHS to rapidly identify those assets, systems, networks, or functions at greatest risk in different situations. For example, the information may be used to quickly identify those assets, systems, networks, or functions that may be the subject of emergent terrorist statements or interest or that may be located in the area of greatest impact from natural disasters.

This information is needed not only to help manage steady-state CI/KR protection and resiliency approaches, but also to inform and support the response to a wide array of incidents and emergencies. Risk may change based on many factors including damage resulting from a natural disaster; seasonal or cyclic dependencies; and changes in technology, the economy, or the terrorist threat. The inventory is used to support domestic incident management by helping to inform decisionmaking; establish strategies for response; and identify priorities for restoration, remediation, and reconstruction.

Currently, this inventory is maintained in the NADB. SSAs and DHS work together and in concert with State, local, and tribal governments, and private sector security partners to ensure that the inventory data structure is accurate, current, and secure. DHS provides guidelines concerning information needed to develop and maintain the inventory. Owners, operators, infrastructure data source managers, and other security partners generally have the best knowledge of their assets, systems, networks, functions, and related data. These subject matter experts work with DHS and the SSAs to deter-

mine the specific information required to support sector and national-level risk analysis. Judgments on the information to be provided for DHS use is informed by a screening process (described in section 3.3.2.2). The screening process applies an essential needs test that considers the consequences that would result if an asset, system, network, or function were lost, exploited, damaged, or disrupted.

For sectors with identifiable facilities, a bottom-up, asset-based approach often is most appropriate for collecting and organizing inventory information; for sectors with virtual- or information-based core processes, a top-down system-, network-, or function-based approach may be more appropriate. A bottom-up approach normally includes an aggregate assessment at the individual facility level; this is with regard to both on-site and off-site consequences to the facility’s mission and the surrounding population that could result from natural disasters, accidents, or terrorist attacks. A top-down approach normally includes an assessment of key missions and the identification of the high-level processes, capabilities, and functions on which those missions depend; it considers dependencies on other sectors to evaluate resiliency, redundancy, and recoverability. Both the top-down and bottom-up approaches recognize that effects on customers, key users, and the public must be considered in the assessment process to understand what is critical.

Information included in the inventory comes from a variety of sources, such as:

- **Sector inventories:** SSAs maintain close working relationships with owners and operators, SCCs, and other sources that maintain inventories necessary for the sector’s business or mission. SSAs provide relevant information to DHS and update it on a periodic basis to ensure that sector assets and critical functions are adequately represented, and that sec-

tor and cross-sector dependencies and interdependencies can be identified and analyzed;

- **Voluntary submittals from security partners:** Owners and operators; State, local, and tribal governments; and Federal departments and agencies voluntarily submit information and previously completed inventories for DHS to consider;
- **Results of studies:** Various government or commercially owned databases developed as the result of studies undertaken by trade associations, advocacy groups, and regulatory agencies may contain relevant information;
- **Periodic data calls:** DHS, in cooperation with SSAs and other security partners, may conduct data calls requesting the voluntary provision of specific information; and
- **Ongoing reviews of particular locations where risk is believed to be higher:** DHS- and SSA-initiated site assessments provide information on vulnerability; help to identify assets, systems, and networks and their dependencies, interdependencies, and critical functionality; and quantify their value relative to the potential consequences of an attack.

DHS, in coordination with SSAs, State and local governments, private sector owners and operators, and other security partners, uses consistent reporting methods to gather appropriate basic information for a range of assets, systems, networks, and critical functions in each sector. This approach relies on existing inventories at the State and local levels to avoid duplication of past efforts. To help ensure currency and accuracy, DHS documents the sources of the information maintained in the inventory. DHS also coordinates with security partners, as needed, to gather additional information for assets, systems, networks, and functions that, based on an initial screening, DHS determines to be potentially nationally critical. This additional information may include:

- System components that are central to the infrastructure mission and function;
- Dependencies and interdependencies (i.e., what an asset depends on in order to function, and which assets are reciprocally dependent upon it);
- Specific information on the asset, system, network, or function needed to support consequence analysis; and
- Assessment information that would enable DHS to conduct further comparative risk analysis in cooperation with the SSAs, the private sector, other security partners, or subject matter experts.

3.2.2 Protecting and Accessing Inventory Information

The Federal Government recognizes the sensitive, business, or proprietary nature of much of the information to be included in the NADB. DHS is responsible for protecting this information from unauthorized disclosure or use. Submissions of asset information for inclusion in the NADB are protected from unauthorized disclosure or use to the maximum extent allowed under applicable Federal, State, or local regulation, including PCII and security classification rules (see section 4.3). Additionally, DHS ensures that all data and licensing restrictions are enforced. DHS has implemented resilient and redundant security measures that apply to the NADB; these provide for system integrity and security, software security, and protection of the data therein.

Access to the NADB is tightly controlled using relevant security clearances and classification guidelines. All users must apply for and be approved for access to the NADB based on appropriate authorization, clearance, and a need to know. Once this information is submitted, DHS verifies clearances and need to know, and assigns each individual role-based access authorization based on the scope of the information requested and required.

3.2.3 SSA Roles in Inventory Development and Maintenance

The specific processes that SSAs use to collect asset, system, and network data; to identify critical functionality; and to coordinate with DHS are described in the individual SSPs. The SSPs include descriptions of mechanisms for making data collection efforts more manageable, such as:

- Prioritizing the approach for data outreach to different security partners;
- Identifying assets, systems, networks, or functions of potential national-, regional-, or sector-level importance;
- Identifying, reviewing, and using existing databases;
- Supporting State, local, and tribal entities in gathering information by helping them identify the types of information most relevant to the protection of potentially high-risk infrastructure; and
- Identifying specific assets, systems, or networks, or classes of assets, systems, or networks, for which additional data collection is unnecessary because of the inherently low risk associated with them.

SSAs help identify and obtain appropriate data for assets, systems, networks, and functions that play a vital role in the Nation's security or economy, particularly those that involve significant dependencies, interdependencies, or critical functionality. For example, a small manufacturer of pharmaceuticals or vaccines could be the sole U.S. manufacturer of that product. Similarly, virtual networks, known only to the owner and operator of a communications service, could provide the only sufficiently capable link between the military and the producer of a defense system component. The identification of less visible assets makes the effort more time-consuming; however, it is a crucial part of the process if a true national risk profile is to be developed. More details on SSA roles and responsibilities, as well as those of other security partners, in creating and maintaining the national CI/KR inventory are contained in appendix 3C.

3.2.4 State Roles in Inventory Development and Maintenance

States often have access to sector-specific information maintained by State regulatory agencies that may be appropriate for use in a national CI/KR inventory. States also may have developed CI/KR inventories in conjunction with other responsibilities, such as incident management and response, economic development, and the oversight of commerce and communications. Because of their CI/KR-related responsibilities and authorities, States provide information that is essential in helping to identify and obtain data about assets, systems, and networks that relate to cross-sector matters.

The State homeland security programs should include descriptions of mechanisms that align with those outlined for the SSAs (see section 3.2.3) and that make data collection efforts more manageable. Additional information on State roles and responsibilities in this area is contained in appendix 3C.

3.2.5 Identifying Cyber Infrastructure

The NIPP addresses the protection of the cyber elements of CI/KR in an integrated manner rather than as a separate consideration. As a component of the sector-specific risk assessment process, cyber infrastructure (assets, systems, networks, and functions) should be identified individually or included as a cyber element of a larger asset, system, or network's description if they are associated with one. The identification process should include information on international cyber infrastructure with cross-border implications, interdependencies, or cross-sector ramifications. The following list

provides examples of cyber assets, systems, or networks that exist in most, if not all, sectors:

- **Business Systems:** Cyber systems used to manage or support common business processes and operations. Examples of business systems include Enterprise Resource Planning, e-commerce, e-mail, and R&D systems.
- **Control Systems:** Cyber systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. Control systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of control systems include SCADA, Process Control Systems, and Distributed Control Systems.
- **Access Control Systems:** Cyber systems allowing only authorized personnel and visitors physical access to defined areas of a facility. Access control systems provide monitoring and control of personnel passing throughout a facility by various means, including electronic card readers, biometrics, and radio frequency identification.
- **Warning and Alert Systems:** Cyber systems used for alerting and notification purposes in many security missions, including homeland security. These systems pass critical information that triggers protection and response actions for formal organizations and individual citizens. Examples include local phone-based hazard alerting systems used by some local governments and the Emergency Alert System established by the Federal Communications Commission (FCC), and its National Oceanic and Atmospheric Administration Weather Radio, which is an all-hazards alerting system provided by the Department of Commerce.

The Internet has been identified as a key resource comprised of domestic and international assets within both the Information Technology and Telecommunications sectors, and is used by all sectors to varying degrees. While the availability of the service is the responsibility of both the Information Technology and Telecommunications sectors, the need for access to and reliance on the Internet is common to all sectors.

DHS supports SSAs and other security partners by developing tools and methodologies to assist in identifying cyber assets, including those that involve multiple sectors. As needed, DHS works with sector representatives to help identify cyber infrastructure within the NIPP risk management framework. For example, DHS collaborates with the Department of Education in addressing cyber protection and resiliency for schools.

3.2.6 Identifying Positioning, Navigation, and Timing Services

Space-based and terrestrial positioning, navigation, and timing services are a component of multiple CI/KR sectors. These services underpin almost every aspect of transportation across all its various modes. Additionally, the Banking and Finance, Telecommunications, Energy, and Water sectors rely on GPS as their primary timing source. The systems that support or enable critical functions in the CI/KR sectors should be identified, either as part of or independent of the infrastructure, as appropriate. Examples of CI/KR functions that depend on positioning, navigation, and timing services include: aviation (navigation, air traffic control, surface guidance); maritime (harbor, inland waterway vessel movement); surface transportation (rail, hazmat tracking); communications networks (global fiber and wireless networks); and power grids.

3.3 Assess Risks

Various methodologies are available to facilitate risk assessment. Many owners and operators use a risk assessment methodology as a component of their business continuity and disaster mitigation planning. A common approach based on a robust understanding of existing methodologies is needed to enable the setting of protection priorities across sectors. The first element of this approach is to establish a common definition and process for analysis of the basic factors of risk for CI/KR protection. In the context of homeland security, the NIPP framework assesses risk as a function of consequence, vulnerability, and threat:

$$R = f(C,V,T)$$

- **Consequence:** The negative effects on public health and safety, the economy, public confidence in institutions, and the functioning of government, both direct and indirect,

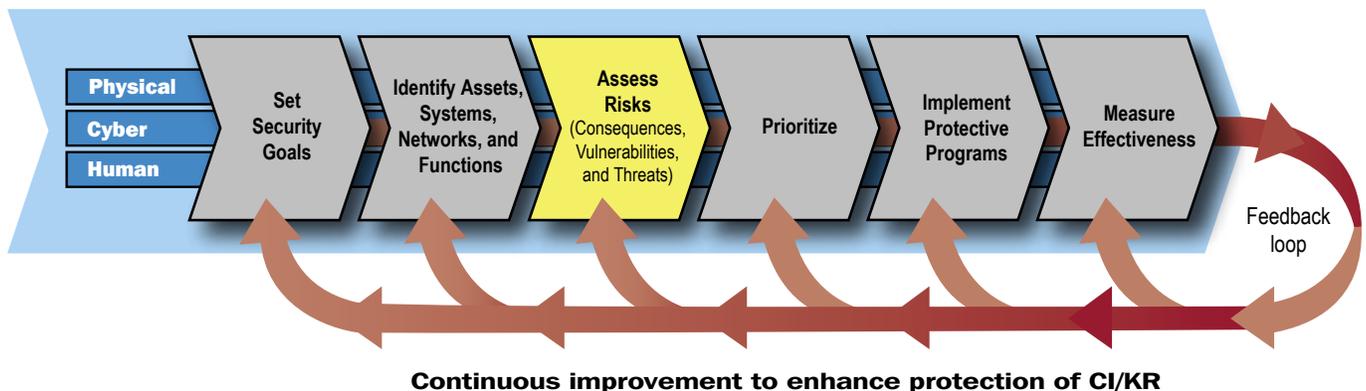
that can be expected if an asset, system, or network is damaged, destroyed, or disrupted by a terrorist attack, natural disaster, or other incident;

- **Vulnerability:** The likelihood that a characteristic of, or flaw in, an asset, system, or network’s design, location, security posture, process, or operation renders it susceptible to destruction, incapacitation, or exploitation by terrorist or other intentional acts, mechanical failures, and natural hazards; and
- **Threat:** The likelihood that a particular asset, system, or network will suffer an attack or an incident. In the context of risk from terrorist attack, the estimate of this is based on the analysis of the intent and the capability of an adversary; in the context of natural disaster or accident, the likelihood is based on the probability of occurrence.

Risk assessments for CI/KR protection consider all three components of risk and are conducted on an asset, system, network, or function basis, depending on the fundamental characteristics of the infrastructure being examined. For some sectors, particularly those with specifically identifiable facilities that might be exploited, an asset-based approach is typically used; for others, particularly those with virtual- or information-based core processes, assessing system or network risk and resiliency is more appropriate.

Once the three components of risk—consequence, vulnerability, and threat—have been assessed for a given asset, system, or network by sector, region, or nationally, they are factored numerically and combined mathematically to give an estimate of the expected loss considering the likelihood of an attack or other incident. Calculating a numerical risk score using comparable, credible methodologies provides a systematic and comparable estimate of risk that can help inform national and sector-level risk management decisions.

Figure 3-4: NIPP Risk Management Framework: Assess Risks



DHS works with the SSAs, State and local governments, private industry, and other security partners to develop an approach that allows risk-based comparisons across sectors, while leveraging assessments and analyses that have already been performed. This approach involves two parallel, mutually supportive efforts:

- Reconfiguring existing, widely used methodologies, or identifying clear and understandable means for making the results of assessments performed using those methodologies comparable with minimal additional cost to security partners; and
- Collaboratively developing a risk assessment process and methodology generally applicable across all sectors that owners and operators will be encouraged to use on a voluntary basis. Owners and operators who might find voluntary use advantageous are those who:
 - Have not previously performed a thorough risk assessment;
 - Wish to streamline their communications with other security partners;
 - Need to update a previously completed assessment; or
 - Would like to use the primary DHS methodology because of the level of support that is available from DHS.

The NIPP establishes baseline criteria for risk assessment methodologies. These criteria provide a guide for improving existing methodologies or modifying them so the investment and expertise they represent can be used to support national-level, comparative risk assessment, planning, and resource prioritization.

DHS is sponsoring the development of a suite of tools based on the Risk Analysis and Management for Critical Asset Protection (RAMCAP) framework that satisfies the baseline criteria for risk assessment and can be used for national cross-sector risk assessment. This tool set enables owners and operators to calculate potential consequences and vulnerability to an attack using a consistent system of measurements. It will also provide the means to convert and compare the results obtained from assessments performed with other suitable methodologies that are consistent with the NIPP baseline criteria.

The NIPP baseline criteria are set forth in the next section. The processes for assessing, analyzing, and combining the three specific components that make up risk—consequence, vulnerability, and threat—are explained in the following

sections. More details regarding the baseline criteria are included in appendix 3A.

3.3.1 NIPP Baseline Criteria for Assessment Methodologies

Many owners and operators regularly perform vulnerability or risk assessments on the assets, systems, and networks under their control. To take advantage of this existing body of work, DHS plans to make every effort to use the results from previously performed assessments wherever possible. However, it should be noted that work on assessments to date has varied widely both within and across sectors in terms of assumptions, comprehensiveness, objectivity, and the inclusion of threat and consequence considerations, as well as information regarding physical/cyber dependencies and interdependencies.

3.3.1.1 Ensuring That Previous Assessments Can Be Used

To be accepted by DHS, existing risk assessment tools and methodologies are reviewed against the NIPP baseline criteria. This review helps ensure that the tools provide results that are suitable for national-level risk analysis, which relies on assessments that are comparable both within and across sectors. DHS and the SSAs will work with security partners to ensure that risk assessment tools and methodologies that are compatible with the NIPP criteria are available to security partners. DHS will leverage and incorporate work already done, to the greatest extent possible, and will help tailor existing tools to meet the baseline criteria as required.

3.3.1.2 Baseline Criteria

The NIPP baseline criteria for assessment methodologies fall into two groups; these criteria are described below and listed specifically in appendix 3A.

The first group provides factors to ensure that the methodology is *credible* to users of the resulting analysis. To be considered credible, a methodology must have a sound basis (it must have integrity); be complete; be based on assumptions and produce results that are defensible; and specifically address the three variables of the risk calculus: consequences, vulnerability, and threat.

The second group ensures that the methodology supports a comparative sector or national risk assessment. To be comparable, a methodology must be documented, transparent, reproducible, and accurate. The methodology must also provide clear and sufficient documentation of the analysis process and the products that result from its use.

3.3.2 Consequence Analysis

The potential consequences of any incident, including terrorist attacks and natural or manmade disasters, is the first factor to be considered in risk assessment. In the context of the NIPP, consequence is measured as the range of loss or damage that can be expected.

The consequences that are considered for the national-level comparative risk assessment are based on the criteria set forth in HSPD-7. These criteria can be divided into four main categories:

- **Human Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries);
- **Economic Impact:** Direct and indirect effects on the economy (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);
- **Impact on Public Confidence:** Effect on public morale and confidence in national economic and political institutions; and
- **Impact on Government Capability:** Effect on the government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

A full consequence assessment takes into consideration public health and safety, economic, psychological, and government impacts; however, estimating potential indirect impacts requires the use of assumptions and other complex variables. An assessment of all categories of consequence may be beyond the capabilities available for a given risk analysis. At a minimum, assessments should focus on the two most fundamental impacts: the human and the most relevant direct economic impact.

3.3.2.1 Consequence Assessment Methodologies That Enable National Risk Analysis

DHS works with SSAs and other security partners to examine the inherent characteristics of assets, systems, or networks to identify worst-case consequences that are likely to result if the CI/KR in question is destroyed, incapacitated, or exploited. The use of common terminology and metrics when assessing consequences supports comparative risk analysis at the national level. DHS works with security partners to develop consequence assessment methodologies that can be applied to a variety of asset, system, or network types and produce comparable quantitative consequence estimates. DHS is working with industry partners to develop

a framework for consequence assessment methodologies for selected CI/KR sectors and subsectors. When fully developed and implemented, the methodologies developed under the RAMCAP framework will provide quantitative results that can be compared to the results of any other RAMCAP consequence assessment, regardless of asset type.

Consequence analysis should address both direct and indirect effects. Many assets depend on multiple inputs to maintain functionality. For example, nearly all sectors rely on the Energy, Information Technology, Telecommunications, Banking and Finance, and Transportation sectors. In some cases, a failure of an asset in one sector can have a significant impact on the ability of an asset in the same or another sector to perform necessary functions. As a result, comprehensive consequence analysis addresses both CI/KR dependency (reliance on another asset or sector for functionality) and CI/KR interdependency (when two or more assets depend on one another) for the purposes of NIPP risk assessment.

Various Federal and State entities, including national laboratories, are developing sophisticated models and simulations to identify dependencies and interdependencies within and across sectors. The Federal Government established the National Infrastructure Simulation and Analysis Center (NISAC) to support these efforts. The NISAC is chartered to develop advanced modeling, simulation, and analysis capabilities for the Nation's CI/KR. These tools address physical and cyber dependencies and interdependencies in an all-hazards context. These sophisticated models enhance the Nation's understanding of CI/KR dependencies and interdependencies, and better inform decisionmakers in the areas of policy analysis, investment, prevention and mitigation planning, education, training, and crisis response.

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

3.3.2.2 Consequence Screening

Many risk assessment methodologies use a simplified and inexpensive-to-use consequence screening, or top-screens, to help owners and operators decide whether a full risk assessment is necessary. For example, DHS uses sector-specific top-screens as part of the RAMCAP framework. This approach allows CI/KR owners and operators to identify their projected level of consequence based on the nature

of their business, proximity to significant populations or other CI/KR, relative importance to the national economy or military capability, and other similar factors. The screening process uses a standard form containing a few simple questions. If this initial screening determines that an attack on an asset, system, or network is likely to result in consequences that are considered low from a national perspective, owners and operators will not be asked to provide additional information to DHS or SSAs. However, assets, systems, or networks that are screened out because of their relatively low national risk may be considered critical on a sector or jurisdictional basis (e.g., a chemical facility that is the primary employer in a given community). Accordingly, additional analysis may be warranted. Owners and operators of CI/KR that are screened out using a consequence screening assessment should consider whether their assets, systems, or networks require more detailed assessments in conjunction with other State, regional, or local CI/KR protection efforts.

3.3.3 Vulnerability Assessment

Vulnerabilities are the characteristics of an asset, system, or network's design, location, security posture, process, or operation that render it susceptible to destruction, incapacitation, or exploitation by mechanical failures, natural hazards, terrorist attacks, or other malicious acts. They identify areas of weakness that could result in consequences of concern, taking into account intrinsic structural weaknesses, protective measures, resiliency, and redundancies.

The vulnerability assessment process typically consists of the following key steps:

- Determining an appropriate vulnerability assessment strategy (e.g., self-assessment, State- or federally led assessment, expert reviews, or independent third-party assessment);
- Identifying a methodology/tool appropriate for the particular type of asset, system, or network under consideration;
- Identifying and grouping vulnerabilities using common threat scenarios;
- Identifying dependencies and interdependencies with other assets and sectors;
- Considering vulnerabilities associated with physical, cyber, and human elements;
- Analyzing benefits of existing protective programs; and
- Assessing residual gaps to determine unresolved vulnerabilities.

3.3.3.1 Vulnerability Assessment Methodologies That Enable National Risk Analysis

Many different vulnerability assessment approaches are used by the different CI/KR sectors. The primary vulnerability assessment methodologies used in each sector are described in the respective SSPs. The SSPs also provide specific detail regarding how the assessments can be carried out (e.g., by whom, how often).

The results of vulnerability assessments need to be comparable in order to support further national-level, cross-sector analysis. DHS, in conjunction with various security partners, continuously improves vulnerability methodologies developed under the RAMCAP framework. This provides two means for producing comparable vulnerability assessment results. First, as part of the framework, DHS develops sector-specific Security Vulnerability Assessment (SVA) modules for individual sectors and subsectors. These SVA modules use a common approach that produces results that may be compared with other SVA module assessment results. Second, as part of the development of each SVA module, DHS and its security partners review vulnerability assessment methodologies that are used in the specific sector or subsector, and assess their compatibility with the NIPP baseline criteria. If methodologies conform to the baseline criteria, then DHS can use assessment results produced using that methodology to support national comparative risk analysis. If the methodologies differ, DHS will work with security partners to either identify ways to adjust the methodology to conform to the NIPP baseline criteria, or will develop "translators" to convert results developed with those methodologies into results that are comparable with the SVA modules. The specific approach will depend on the degree of difference and the robustness of the method in question.

3.3.3.2 SSA and DHS Analysis Responsibilities

SSAs and their security partners are responsible for taking stock of, and facilitating, vulnerability assessment activities within their sectors; owners or operators typically perform these assessments. SSAs are also responsible for compiling, where possible, vulnerability assessment results for use in sector and national risk management efforts. Vulnerability assessment information may be submitted under the PCII Program (see Section 4.3, Protection of Sensitive CI/KR Information). SSAs are responsible for working with DHS to validate the results of those assessments for assets that are of the greatest concern from the sector perspective. SSAs should involve owners and operators in this review whenever possible.

DHS is responsible for ensuring that comprehensive vulnerability assessments are performed for CI/KR that is deemed

nationally critical. This may involve DHS experts performing the vulnerability assessment in conjunction with the CI/KR owner or operator, or working with the CI/KR owner or operator, the SSA, or a third-party auditor to perform or to verify previously performed assessments.

DHS also conducts or supports vulnerability assessments that address the specific needs of the NIPP's comprehensive approach to CI/KR protection. Such assessments may:

- More fully investigate dependencies and interdependencies within and between sectors;
- Serve as a basis for developing common vulnerability reports that can help identify strategic needs for protective programs or R&D across sectors or subsectors;
- Fill selected gaps when sectors or owners or operators have not yet completed assessments and such studies are needed immediately; and
- Test and validate new methodologies or streamlined approaches for assessing vulnerability.

In some sectors and subsectors, vulnerability assessments have never been performed or may have been performed for only a small number of high-profile or high-value assets, systems, or networks. To help assist in closing this gap, DHS works with SSAs, and owners and operators, as well as other security partners, as appropriate, to determine common criteria for vulnerability assessments and provides:

- Vulnerability assessment tools that may be used as part of self-assessment processes;
- Informative reports for industrial sectors, classes of activities, and high-consequence or at-risk special event sites;
- Generally accepted risk assessment principles for major classes of activities and high-consequence or at-risk special event sites;
- Assistance in the development and sharing of industry-based standards and tools;
- Recommendations regarding the frequency of assessments, particularly in light of emergent threats;
- Site assistance visits and vulnerability assessments of specific CI/KR of particular concern as requested by owners and operators; and
- Cross-sector cyber vulnerability assessment best practices.

3.3.4 Threat Analysis

The remaining factor to be considered in the NIPP risk assessment process is the analysis of threat. In the context of terrorist risk assessment, the threat component of the analysis is calculated based on the likelihood of a terrorist attack method on a particular asset, system, or network.¹⁹ The estimate of this likelihood is based on an analysis of intent and capability of a defined adversary, such as a terrorist group. In the context of a natural disaster or accident, the likelihood is based on the probability of occurrence. The incident management, disaster response, public safety, and other communities have developed and use various tools to estimate the threat of natural disasters and accidents. These tools include such analytical aids as the models used by the NHC to forecast hurricane landfall and the fault tree models used by the NRC in nuclear power plant engineering analysis. Because similar models are not yet in broad use for terrorist threats, the NIPP provides an augmented framework for the terrorist aspects of threat analysis.

Assessment of the current terrorist threat to the United States is derived from extensive study and understanding of terrorists and terrorist organizations, and frequently is dependent on analysis of classified information. DHS, to the greatest extent possible, provides its security partners with Federal Government-coordinated unclassified assessments of potential terrorist threats and appropriate access to classified assessments where necessary. These threat assessments are derived from analysis of adversary intent and capability, and describe what is known about terrorist interest in particular CI/KR sectors, as well as specific attack methods. Since international terrorists, in particular, have continually demonstrated flexibility and unpredictability, DHS and its partners in the Intelligence Community also analyze known terrorist goals and capabilities to provide CI/KR owners and operators with a broad view of the potential threat and postulated terrorist attack methods.

3.3.4.1 Key Aspects of the Terrorist Threat to CI/KR

Analysis of terrorist goals and motivations identify domestic and international CI/KR as potentially prime targets for terrorist attack; given the deeply rooted nature of these goals and motivations, CI/KR likely will remain a highly attractive target for terrorists for some time to come. The characteristics of each of the elements of CI/KR—physical, cyber, and human—relate to attack modalities that risk-mitigation measures must address. Physical attacks, including the exploitation of physical elements of CI/KR, represent the attack method most frequently used overtly by terrorists.

¹⁹ In calculations for risk analysis, the term “threat” is an estimated value that approximates the likelihood that a specific asset, system, network, sector, or region will suffer an attack or an incident. This differs from “threat scenarios,” or “threat analysis,” which are generalized descriptions of potential methods of attack that are used to help inform consequence and vulnerability assessments.

In addition to physical attacks, terrorists may use the cyber domain as a platform to attack America's CI/KR. The use of innovative technology and interconnected networks in CI/KR operations improves productivity and efficiency, but also may increase the Nation's risk to cyber attacks. Because of the interconnected nature of the cyber elements of CI/KR, cyber attacks can spread quickly and could have a substantial impact on the Nation's essential services and functions. Credible information on specific adversaries or attack modalities frequently is not available in the context of cyber threats. However, the rapidly changing technology and the relatively easy access to and use of powerful cyber tools raises the likelihood that adversaries can develop the capability to conduct cyber attacks against CI/KR. Cyber threats are addressed in unclassified documents such as the *National Strategy to Secure Cyberspace* as well as classified reports such as the *National Intelligence Estimate of Cyber Threats to the U.S. Information Infrastructure*.

A third important aspect in this element of risk is the long-standing threat posed by insiders, or persons who have access to sensitive information and facilities. Insider threats can result from intentional actions, such as infiltration of the organization by terrorists, or unintentional actions, such as employees who are exploited or unknowingly manipulated to provide access to, or information about, CI/KR. Insiders can intentionally compromise the security of CI/KR through espionage, sabotage, or other harmful acts motivated by the rewards offered to them by a terrorist or other party. Others may provide unwitting assistance to an insider threat through lack of awareness of the need for or methods to protect assets or employees (e.g., by leaving security badges and uniforms in open areas). CI/KR owners and operators and authorities with protection responsibilities screen and, if necessary, monitor employees in sensitive positions. These efforts often benefit from the support of Federal regulations and programs that relate to security clearances, and employment-related screening. Examples include industrial security clearance programs, managed by DOD, and screening for personnel afforded unescorted access to commercial aircraft or secure areas at airports, overseen by the Transportation Security Administration (TSA).

3.3.4.2 Homeland Infrastructure Threat and Risk Analysis Center

The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) conducts integrated threat analysis for all CI/KR sectors. As called for in section 201 of the Homeland Security Act, HITRAC brings together intelligence and infrastructure specialists to ensure a complete and sophisticated

understanding of the risks to U.S. CI/KR. HITRAC works in partnership with the U.S. Intelligence Community and national law enforcement to integrate and analyze intelligence and law enforcement information on the threat. It also works in partnership with the SSAs and owners and operators to ensure that their expertise on infrastructure operations is integrated into threat analysis. This coordination is carried out through a number of mechanisms, including the use of liaison personnel from the private sector, the use of on-call subject matter experts, and coordination with existing organizations such as National Coordinating Center for Telecommunications (NCC) and the SCCs or Information Sharing and Analysis Centers (ISACs) discussed in chapter 4.

As shown in figure 3-5, HITRAC develops analytical products by combining intelligence expertise based on all-source information, threat assessments, and trend analysis with practical business and CI/KR operational expertise informed by current infrastructure status and operations information. This comprehensive analysis provides an understanding of the threat, CI/KR vulnerabilities, the potential consequences of attacks, and the effects of risk-mitigation actions on not only the threat, but also on business and operations. This combination of intelligence and practical knowledge allows HITRAC to provide CI/KR risk assessment products that contain strategically relevant and actionable information. It also allows HITRAC to identify intelligence collection requirements in conjunction with owners and operators so that the intelligence community can provide the type of information necessary to support the CI/KR protection mission. HITRAC coordinates closely with security partners outside the Federal Government through the SCCs, GCCs, and ISACs to ensure that its analytic products are relevant to security partner needs, and that they are accessible to the partners who need them.

Based on HITRAC analysis, DHS produces two classes of information that support the NIPP:

- Information that supports responses to emergent threats or immediate incidents; and
- Information that supports the strategic planning needed to enhance the protection of U.S. CI/KR over the long term.

Each of these classes of information and the specific DHS products that they include are discussed below.

Threat and Incident Information: DHS leverages 24/7 intelligence and operations monitoring and reporting from multiple sources to provide analysis that is based on the most current information available on threats, incidents, and infra-

structure status. Real-time analysis of threat, situation, and CI/KR status information provided by DHS is of unique value to security partners and helps them determine if changes are needed in steady-state CI/KR risk management measures.

Specialized products that directly support the NIPP and SSPs include incident reports and threat warnings, which are made available to appropriate security partners.

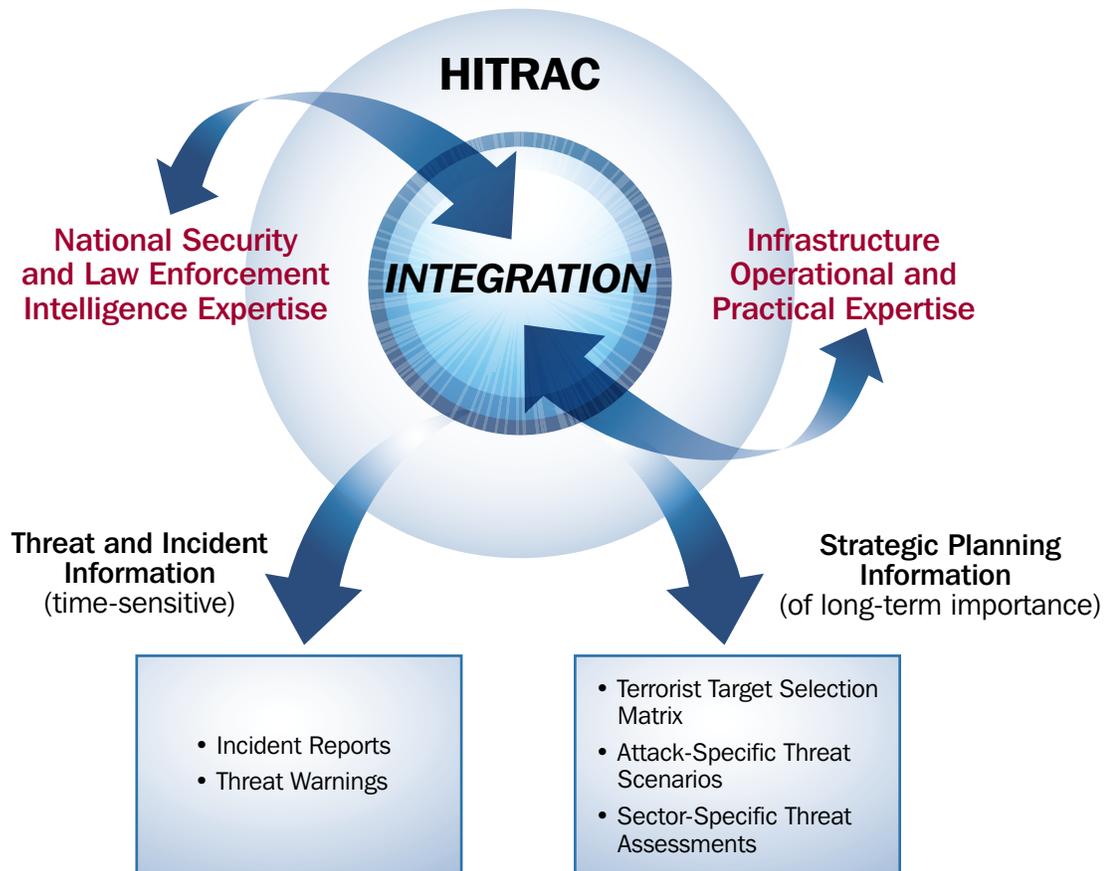
- **Incident Reports:** DHS monitors information on incidents to provide reports that CI/KR owners and operators and other decisionmakers can use with confidence when considering how evolving incidents might affect their security posture. This reporting provides a responsive and credible source to verify or expand on information that security partners may receive initially through news media, the Internet, or other sources. DHS works with multiple government and private sector operations and watch centers to combine situation reports from law enforcement, intelli-

gence, and private sector sources with infrastructure status and operational expertise to rapidly produce reports from a trusted source. These help inform the decisions of owners and operators regarding changes in risk-mitigation measures that are needed to respond to incidents in progress, such as rail or subway bombings overseas that may call for precautionary actions domestically.

- **Threat Warnings:** DHS fuses all-source information to provide analysis of emergent threats on a timely basis. Many of the indicators that are reported by intelligence or law enforcement are not associated with an incident in progress, but are the product of careful intelligence collection. Such indicators also may be of significance only when interpreted in the context of infrastructure operational or status information. DHS monitors the flows of intelligence, law enforcement, and private sector security information on a 24/7 basis in light of the business, operational,

Figure 3-5: Threat Analysis Combines Intelligence and Infrastructure Expertise to Provide Threat and Incident Information and Strategic Planning Information

Threat Analysis Tools and Information



and status expertise provided by its owner and operator security partners to produce relevant threat warnings for CI/KR protection. This analysis clarifies the implications of intelligence reporting about targeted locations or sectors, potential attack methods and timing, or the specific nature of an emerging threat.

- **Strategic Planning Information:** HITRAC analyzes information about terrorist goals, objectives, and attack capabilities to assess the potential terrorist attack profiles that might be used against each CI/KR sector. This provides the best-informed estimate of the potential threat, and is used as a supplement to, or in the absence of, specific intelligence and warnings regarding particular targets, attack vectors, or timing. This analysis provides decisionmakers with the broad, analytically based information on the threat that is necessary to inform investment priorities and program design in conjunction with strategic planning. It also provides the overarching analytic foundation for incident reports and threat warnings produced by DHS and other Federal partners.

HITRAC also develops specialized products for strategic planning that directly support the NIPP and SSPs. These products include a terrorist target selection matrix, which outlines plausible means of attack for each of the CI/KR sectors, a catalog of attack-specific scenarios, and a sector-specific threat report that provides detailed information on the estimated threat facing each sector. In addition to these specific products, HITRAC produces special, longer term strategic assessments and trends analyses that help define the evolving threat to the Nation's CI/KR.

- **Terrorist Target Selection Matrix:** DHS provides threat assessments to SSAs, CI/KR owners and operators, and other security partners who require them. It uses the Terrorist Target Selection Matrix produced by HITRAC as an analytical tool for identifying which sectors are potentially prone to different terrorist attack modalities.

The matrix maps terrorist goals and objectives against an array of possible attack modalities on a sector-by-sector basis. If intelligence analysis of terrorist intent and capabilities determines that terrorists are unlikely to use particular attack methods against a specific CI/KR sector or subsector, it is noted as an unlikely possibility and further consequence or vulnerability assessment may not be warranted. If a combination is determined to meet only one or two primary terrorist attack objectives, the sector is rated as modestly attractive as a terrorist target. If terrorists can achieve a majority of their objectives by using

a particular attack method against a sector or subsector, the situation warrants careful attention and priority for consequence and vulnerability assessments.

This product supports national-level risk assessments, sector-specific application of the NIPP risk management framework, and development and implementation of the SSPs.

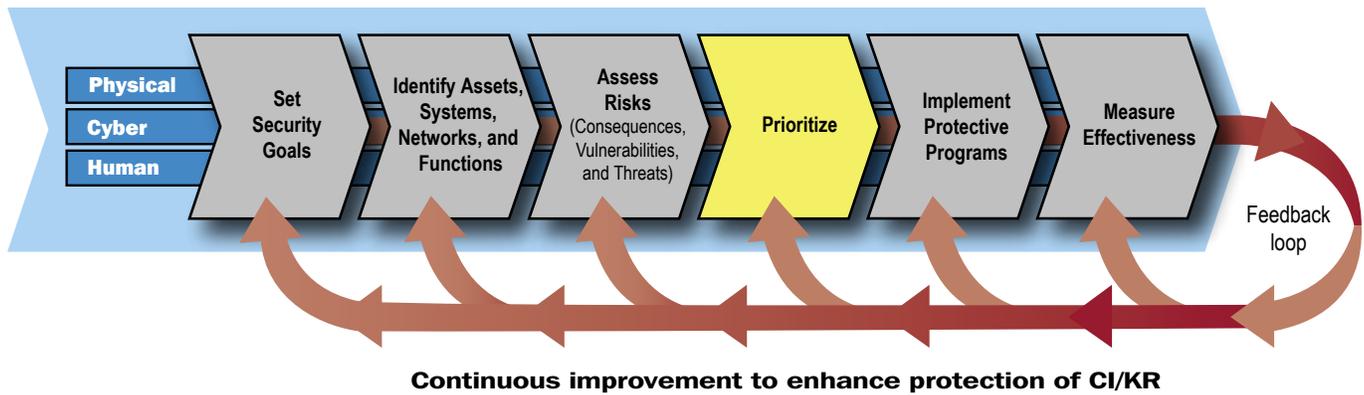
- **Attack-Specific Threat Scenarios:** Attack-Specific Threat Scenarios are detailed vignettes of the specific methods, techniques, and actions terrorists are likely to use to attack specific types of U.S. CI/KR. The scenarios are based on HITRAC analysis of known terrorist capabilities or on their stated intent as derived from intelligence and the study of terrorist tactics, techniques, and capabilities. Threat scenarios are specific enough to be used by corporate or facility-level security officers to support operational security planning.

This product supports facility-level threat surveillance by security forces, owner and operator requests for intelligence information, and risk management action planning. It also provides detailed threat information for the sector-specific threat assessment described below.

- **Sector-Specific Threat Assessment:** DHS uses the information developed for the Terrorist Target Selection Matrix and the Attack-Specific Threat Scenarios to produce Sector-Specific Threat Assessments that provide an overall assessment of the potential terrorist threats posed to each of the CI/KR sectors, as well as an analysis of how these threats relate to sector vulnerabilities and consequences. These assessments include known specific and general terrorist threat information for each sector, as well as relevant background information such as terrorist objectives and motives as they apply to the sector. Each sector-specific report includes the Terrorist Target Selection Matrix for the sector and specifies those Attack-Specific Threat Scenarios that may be relevant to the sector. The assessments are updated on a routine basis to include the most current intelligence findings and operational trends analyses. HITRAC works with each sector to develop and provide threat products that are tailored to meet sector-specific and subsector information needs.

This product is used to support detailed sector-level planning, including SSP development and implementation, and also to provide the detailed threat information necessary for additional security-related planning.

Figure 3-6: NIPP Risk Management Framework: Prioritize



3.4 Prioritize

Prioritization for CI/KR protection is used to focus planning, foster coordination, and support effective resource allocation and incident management, response, and restoration decisions.

The NIPP risk management framework provides the process for developing comparable estimates of the risk relevant to CI/KR. The framework is applicable to risk assessments on an asset, system, network, function, sector, State, regional, or national basis. Comparing the risk faced by different entities helps identify where risk mitigation is most pressing, and to subsequently determine the most cost-effective protective actions, including those related to the cyber and human elements of CI/KR. This identifies which CI/KR should be given priority for protection and which alternative protective actions represent the best investment based on risk. The prioritization process also provides information that can be used during incident response to help inform decisionmakers regarding issues associated with CI/KR restoration.

3.4.1 The Prioritization Process

The prioritization process involves aggregating, combining, and analyzing risk assessment results to determine which assets, systems, networks, functions, sectors, or other relevant groupings face the highest risk. This process leads to a comprehensive picture of risk for the relevant CI/KR groups and allows protection priorities to be established; it also provides the basis for understanding the risk-mitigation benefits that, along with costs, are used to support protection planning and the informed allocation of resources.

This process involves two related activities: The first determines which sectors, regions, or other aggregation of CI/KR assets, systems, networks, or functions are subject to the highest risk as calculated using the NIPP risk management

framework. Those exposed to the greatest risk are accorded the highest priority in risk management program development. The second activity determines which protective actions are expected to provide the greatest mitigation of risk for any given investment. The risk management initiatives that result in the greatest risk mitigation for the investment proposed are accorded the highest priority in program design, resource allocation, budgeting, and implementation. This approach ensures that programs make the greatest contribution possible to overall CI/KR risk mitigation in the context of resources available.

Both of these activities involve translating different risks into common and comparable indices that can be combined and synthesized. The specific mathematical approach to this normalization process is described in other, more detailed guidance documents such as the Risk Analysis Methodology Report prepared by DHS each fiscal year to support the homeland security grants program. Although the procedure is based on a mathematical process, it also involves the judgment and assumptions of risk analysts and decisionmakers. These factors significantly shape the process and are clearly stated and documented to ensure that they are understandable to other security partners and the public.

Assessments become more complex at more aggregate levels, as when comparisons are necessary across sectors. Such assessments rely more heavily on the subjective interpretation of estimates derived from the data that can be collected, as well as differences in assumptions.

3.4.2 Tailoring Prioritization Approaches to Sector Needs

CI/KR security partners rely on different approaches to prioritize risk management activities according to specific sector needs, risk landscapes, security approaches, and busi-

ness environment. For example, asset-based priorities may be appropriate for CI/KR that is facility based, or for assets, systems, or networks that can be exploited and used as weapons. Function-based priorities may more effectively ensure continuity of operations in the event of a terrorist attack or natural disaster in sectors where CI/KR resilience may be more important than CI/KR hardening. Programs to protect assets, systems, or networks give priority to investments that protect physical assets or ensure resilience in virtual systems depending on which option best enables CI/KR risk management.

To ensure a consistent approach to risk analysis for CI/KR protection, security partners establish priorities based on risk analysis that is consistent with the NIPP baseline criteria for risk assessment methodologies; these can be quick-response, top-down assessments using surrogate data or data at high levels of CI/KR aggregation (e.g., functions of population density as a surrogate for casualties), or they can be detailed bottom-up analyses using detailed data on specific individual facilities and employing sophisticated threat models.

3.4.3 The Uses of Prioritization

Prioritization based on risk or the individual components of risk is used for different purposes at several points in the risk management process. For example, in the sharing and collection of risk-related data, top-screening methods based on estimated consequences are used to identify the information that is pertinent to assets, systems, networks, and functions that are essential to business or mission continuity.

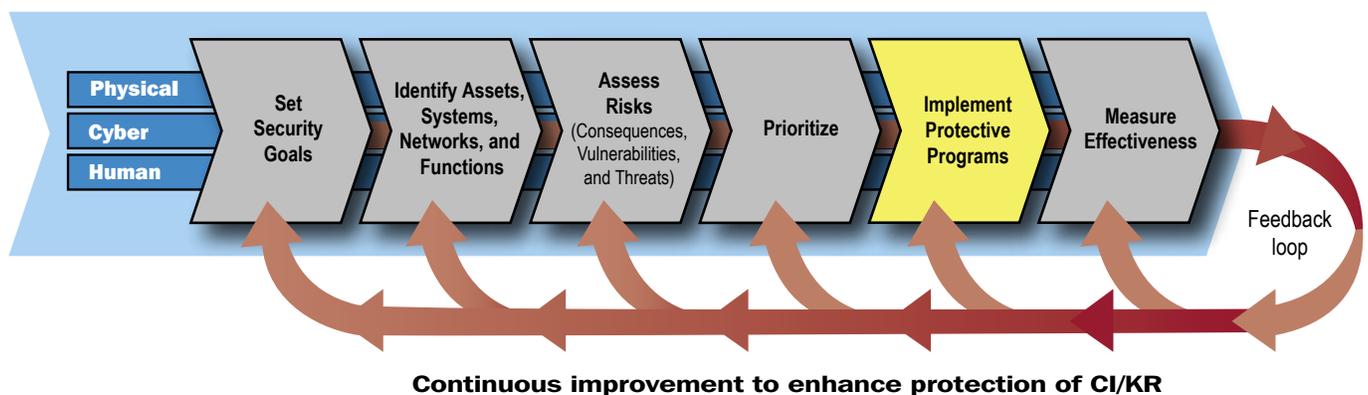
A primary use of prioritization is to inform resource allocation decisions, such as where protection programs should be instituted; the appropriate level of investment in these programs; and which protection measures offer the greatest return on investment. Because resources for CI/KR protection are limited, risk analysis based on empirical information must be completed before sound priorities can be established.

Different possible risk management initiatives involve different degrees of cost and effectiveness. In the design of protection programs and budgets, priority is given to those protective measures that provide the greatest mitigation of risk for the resources that are available. To determine this, security partners designing programs and budgets must evaluate the effect of these different options on reducing or mitigating consequence, vulnerability, or threat. In this process, they combine cost estimates with risk-mitigation estimates in a cost-benefit analysis to choose between the different options, and should consider as wide a range of program options as is practical in making the choice.

At the national level, DHS is responsible for overall national risk-based CI/KR prioritization in close collaboration with the SSAs and other security partners.

The result of the prioritization process is information. This information reflects CI/KR protection and risk-mitigation requirements and provides the rationale and justification for implementing specific programs or actions. Although for some specific purposes, a master inventory of facilities or sites in priority order may be useful, the results of the prioritization process are primarily used in other ways, such as in guidance documents or the decisions underpinning department budget requests. For example, the NADB is not a prioritized list of CI/KR, but rather a database of information on infrastructure assets, systems, and networks that allows analysts to compute risk to help inform decisionmakers in a range of different situations. At the national level, the results of the prioritization process are reflected in a number of guidance documents. These include the Sector CI/KR Protection Annual Reports from the SSAs to the Secretary of Homeland Security and the National CI/KR Protection Annual Report that DHS develops to summarize national CI/KR protection priorities and requirements and to inform the Federal budget process.

Figure 3-7: NIPP Risk Management Framework: Implement Protective Programs



3.5 Implement Protective Programs

The risk assessment and prioritization process enables DHS, SSAs, and other security partners to identify opportunities to enhance current CI/KR protection programs where they will offer the greatest benefit. Security partners give priority in the development of CI/KR protection programs to focus resources on assets, systems, networks, and functions that are deemed to be at the greatest risk.

The risk assessment and prioritization activities within each sector will help identify requirements for current protective programs and shortfalls for future efforts. Some of the identified shortfalls or opportunities for improvement will be filled by owner/operators, either voluntarily or based on various forms of incentives. Other shortfalls will be addressed through the protective programs each sector develops under the SSP or through cross-sector or national initiatives undertaken by DHS.

The Nation's CI/KR is widely distributed in both a physical and logical sense. Effective CI/KR protection requires both distributed implementation of protective programs by security partners, and focused national leadership to ensure implementation of a comprehensive, coordinated, and cost-effective approach that helps to reduce or manage the risks to the Nation's most critical assets, systems, networks, and functions. At the implementation level, protective programs consist of diverse actions undertaken by various security partners. From the leadership perspective, programs are structured to address coordination and cost-effectiveness.

The following sections describe the nature and characteristics of best practice protective programs, as well as some existing programs that could be applied to specific assets, systems, networks, or functions.

3.5.1 Protective Actions

Protective actions involve measures designed to prevent, deter, and mitigate the threat; reduce vulnerability to an attack or other disaster; minimize consequences; and enable timely, efficient response and restoration in a post-event situation, whether a terrorist attack, natural disaster, or other incident. Protective actions vary across a wide spectrum of activities as follows:

- **Deter:** Cause the potential attacker to perceive that the risk of failure is greater than that which they find acceptable. Examples include improved awareness and security (e.g., restricted access, vehicle checkpoints) and enhanced police and/or security officer presence;

- **Devalue:** Reduce the attacker's incentive by reducing the target's value. Examples include developing redundancies and maintaining backup systems or key personnel;
- **Detect:** Identify potential attacks and validate and/or communicate the information, as appropriate. General detection activities include intelligence gathering, analysis of surveillance activities, and trend analysis of law enforcement reporting. For specific assets, examples include intrusion-detection systems, network monitoring systems, operation alarms, surveillance, detection and reporting, and employee security awareness programs; and
- **Defend:** Protect assets by preventing or delaying the actual attack, or reducing an attack's effect on an asset, system, or network. Examples include perimeter hardening by enhancing buffer zones, fencing, structural integrity, and cyber defense tools such as antivirus software.

Protective programs also may include actions that mitigate the consequences of an attack or incident. These actions are focused on the following aspects of preparedness:

- **Mitigate:** Lessen the potential impacts of an attack, natural disaster, or accident by introducing system redundancy and resiliency, reducing asset dependency, or isolating downstream assets;
- **Respond:** Activities designed to enable rapid reaction and emergency response to an incident, such as conducting exercises and having adequate crisis response plans, training, and equipment; and
- **Recover:** Allow businesses and government organizations to resume operations quickly and efficiently, such as using comprehensive mission and business continuity plans that have been developed through prior planning.

Generally, it is considered more cost-effective to build security into assets, systems, and networks than to retrofit them with security measures after initial development. Accordingly, security partners should consider how risk management, robustness, resiliency, and appropriate physical and cyber security enhancements could be incorporated into the design and construction of new CI/KR.

In situations where robustness and resiliency are keys to CI/KR protection, providing protection at the system level rather than at the individual asset level may be more effective and efficient (e.g., if there are many similar facilities, it may be easier to allow other facilities to provide the infrastructure service rather than to protect each facility). Both are possible approaches to meeting NIPP objectives.

3.5.2 Characteristics of Effective Protective Programs

Characteristics of effective CI/KR protective programs include, but are not limited to, the following:

- **Comprehensive:** Effective protective programs must address the physical, cyber, and human elements of CI/KR, as appropriate, and consider long-term, short-term, and sustainable activities. SSPs describe programs and initiatives to protect CI/KR within the sector (e.g., operational changes, physical protection, equipment hardening, cyber protection, system resiliency, backup communications, training, response plans, and security system upgrades).
- **Coordinated:** Because of the highly distributed and complex nature of the various CI/KR sectors, the responsibility for protecting CI/KR must be coordinated:
 - CI/KR owners and operators (public or private sector) are responsible for protecting property, information, and people through measures that manage risk to help ensure more resilient operations and more effective loss prevention. These measures include increased awareness of terrorist threats and implementation of operational responses to reduce vulnerability (e.g., changing daily routines, keeping computer software and virus-checking applications up to date, and applying fixes for known software defects).
 - State, local, and tribal authorities are responsible for providing or augmenting protective actions for assets, systems, and networks that are critical to the public within their jurisdiction and authority. They develop protective programs, supplement Federal guidance and expertise, implement relevant Federal programs (such as the Urban Area Security Initiative or the Buffer Zone Protection Program (BZPP)), and provide specific law enforcement capability as needed. When appropriate, they have access to Federal resources to meet jurisdictional protection priorities.
 - Federal agencies are responsible for enabling or augmenting protection for CI/KR that is nationally critical or coordinating the efforts of security partners and the use of resources from different funding sources. DHS, SSAs, and other Federal departments and agencies carry out these responsibilities while respecting the authorities of State, local, and tribal governments, and the prerogatives of the private sector.
 - SSAs, in conjunction with security partners, provide information on the most effective long-term protective strategies, develop protective programs, and coordinate the implementation of programs for their sectors. For some sectors, this includes the development and sharing of best practices and related criteria, guidance documents, and tools.
- DHS, in collaboration with SSAs and other public and private sector partners, serves as the national focal point for the development, implementation, and coordination of protective programs (including cyber security efforts) for those assets that are deemed nationally critical.
- **Cost-Effective:** Effective CI/KR protective programs seek to use resources efficiently by focusing on actions that offer the greatest mitigation of risk for any given expenditure. The following is a discussion of factors that should be considered when assessing the cost-effectiveness and public benefits derived through implementation of CI/KR protection initiatives:
 - **Operating with full information and lowering coordination costs:** The NIPP describes the mechanisms that enable the use of information regarding threats and corresponding protective actions. It includes information sharing among security partners; provision of a dedicated communications network; and the use of established, interoperable industry and trade association communications mechanisms. The NIPP also helps to lower the cost of coordination through such mechanisms as security partnership arrangements and, where appropriate, the use of a regulatory or incentives-based framework to encourage or drive action.
 - **Addressing the present-future tradeoff in long lead-time investments:** The NIPP provides the processes and coordinating structures that allow State, local, and tribal governments and private sector partners to effectively use long lead-time approaches to CI/KR protection.
 - **Providing for appropriate roles among security partners:** Appropriate roles for CI/KR protection reflect basic responsibilities and shared risks and burdens. CI/KR owners and operators are responsible for protecting property, information, and people through measures that manage risk and help ensure more resilient operations and more effective loss prevention. State, local, and tribal authorities are responsible for providing or augmenting protective actions for assets, systems, and networks that are critical to the public within their jurisdiction and authority. Federal agencies are responsible for coordinating and enabling protection for CI/KR that is nationally critical. They coordinate with regulatory agencies to help

ensure that CI/KR protection issues are fully understood and considered in their deliberations. As discussed in chapter 7, they may make Federal resources available for selected State, local, or tribal CI/KR protection efforts through grant programs in certain circumstances.

- **Matching the underlying economic incentives of each security partner to the extent possible:** The NIPP supports market-based economic incentives wherever possible by relying on security partners to undertake those efforts that are in their own interest and complementing those efforts with additional resources where necessary and appropriate. This coordinated approach builds on efforts that have proven to be effective and that are consistent with best business practices, such as owners and operators selecting the measures that are best suited to their particular risk profile and needs.
- **Addressing the public-interest aspects associated with CI/KR protection:** Protective actions for CI/KR that provide benefits to the public at large go beyond the actions that benefit owners and operators, or even those that benefit the public residing in a particular State, region, or locality. Such additional actions reflect different levels of the public interest—some CI/KR are critical to the national economy and to national well-being; some CI/KR are critical to a State, region, or locality; some CI/KR are critical only to the individual owner/operator or direct customer base. Actions to protect the public’s interest that require investment beyond the level that those directly responsible for protection are willing and able to provide must be of sufficient priority to warrant the use of the limited resources that can be provided from public funding or may require regulatory action or appropriate incentives to encourage the private sector to undertake them.
- **Risk-Based:** Protective programs focus on mitigating risk. Protective actions should be designed to allow measurement, evaluation, and feedback based on risk mitigation. This allows owners, operators, and SSAs to reevaluate risk after the program has been implemented. Protective programs use different mechanisms for addressing each element of risk and combine their effects to achieve overall risk mitigation. These mechanisms include:
 - **Consequences:** Protective programs directly limit or manage consequences by reducing the possible loss resulting from a terrorist attack or other disaster through redundant system design, backup systems, and alternative sources for raw materials or information.

- **Vulnerability:** Protective programs directly reduce vulnerability by decreasing the susceptibility to destruction, incapacitation, or exploitation by correcting flaws or strengthening weaknesses in assets, systems, and networks.
- **Threat:** Protective programs indirectly reduce threat by making assets, systems, or networks less attractive targets to terrorists by lessening vulnerability and lowering consequences. As a result, terrorists are less likely to achieve their objectives and, therefore, less likely to focus on the CI/KR in question.

3.5.3 Protective Programs, Initiatives, and Reports

DHS, in collaboration with SSAs and other security partners, undertakes a number of protective programs, initiatives, activities, and reports that support CI/KR protection. Many of these are available to or provide resources for security partners. These activities span a wide range of efforts that include, but are not limited to, the following:

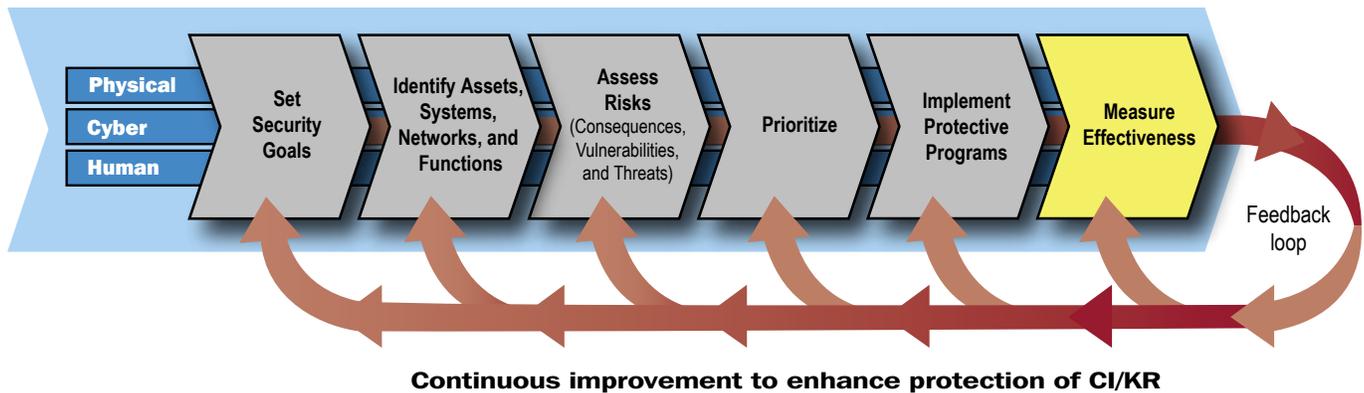
- **Buffer Zone Protection Program:** A grant program designed to provide resources to State and local law enforcement to enhance the protection of a given critical facility.
- **Assistance Visits:** Facility security assessments jointly conducted by a federally led team and facility owners and operators that are designed to facilitate vulnerability identification and mitigation discussions between security partners and individual owners and operators.
- **Training Programs:** Training programs are designed to provide security partners a source from which they can obtain specialized training to enhance CI/KR protection. Subject matter, course length, and location of training can be tailored to security partner needs.
- **Control Systems Security:** DHS coordinates efforts among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors to improve control system security within and across all CI/KR sectors.

A detailed discussion of DHS-supported programs is provided in appendix 3B.

SSAs and other Federal departments and agencies also oversee protective programs, initiatives, and activities that support CI/KR protection. Many of these are also available or provide resources for security partners. Examples include:

- The Department of Veterans Affairs created a methodology also used by the Smithsonian Institution and adapted by

Figure 3-8: NIPP Risk Management Framework: Measure Effectiveness



Federal Emergency Management Agency (FEMA) Manual 452, *Risk Management: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, to assess the risk to and mitigation for hundreds of buildings and museums.

- DOT manages a Pipeline Safety grant program that supports efforts to develop and maintain State natural gas, liquefied natural gas, and hazardous liquid pipeline safety programs.
- HHS is conducting pilot tests that include a tribal hospital, a local substance abuse treatment center, and an owner/operator administrative office in preparation for a vulnerability assessment of more than 4,000 health care-related facilities.

Other protective activities include developing and providing informational reports, such as the DHS Characteristics of Common Vulnerabilities Reports and the Indicators of Terrorist Activity Reports, which are available to all State and Territorial homeland security offices. In addition to threat and vulnerability information, informational reports also include best practices for protection measures. One report in particular, FEMA’s Risk Management Series, addresses the protection of buildings and is applicable across sectors.

3.6 Measure Effectiveness

Measuring effectiveness drives continuous improvement of CI/KR risk-mitigation programs at the sector level and overall program performance at the national level. The NIPP uses a metrics-based system to provide feedback on efforts to attain the goal and supporting objectives articulated in chapter 1. The metrics also provide a basis for establishing accountability, documenting actual performance, facilitating diagnoses,

promoting effective management, and reassessing goals and objectives. Metrics offer a quantitative assessment to affirm that specific objectives are being met or to articulate gaps in the national effort or supporting sector efforts. They enable identification of corrective actions and provide decisionmakers with a feedback mechanism to help them make appropriate adjustments. They can also provide qualitative insights to help make informed decisions. Cost-benefit analyses of programs, lessons learned from exercises, actual incidents, and alerts provide additional objective input into the process.

3.6.1 NIPP Metrics and Measures

3.6.1.1 Measuring Performance

The NIPP risk management framework uses three types of quantitative indicators to measure program performance, to include cost-effectiveness. These indicators span a wide range: descriptive measures are usually the easiest and least costly to collect, but bear only an indirect relationship to the actual performance of CI/KR protection efforts; outcome measures most directly measure performance, but often have limitations due to the need for modeling, assumptions, or complex formulas in calculating them. The NIPP risk management framework relies on a mix of these measures that will change over time as the framework matures and as security partners learn which measures are the most useful in actual practice:

- **Descriptive Measures** are used to understand sector resources and activities; they do not reflect CI/KR protection performance. Examples include the number of facilities in a jurisdiction; the population resident or working within typical incident effects footprints; and the number, nature, and location of suppliers in an infrastructure service provider’s supply chain.

- **Process (or Output) Measures** are used to measure whether specific activities were performed as planned, tracking the progression of a task, or reporting on the output of a process such as inventorying assets. Process measures show progress toward performing the activities necessary to achieve CI/KR protection goals. They also help build a comprehensive picture of CI/KR protection status and activities. Examples include the number of protective programs implemented in a specific fiscal year and the level of investment for each, the number of detection systems installed at facilities in a given sector, the proportion of a facility's workforce that has completed training, and the level of response to a data call for asset information.
- **Outcome Measures** track progress toward a strategic goal by beneficial results rather than level of activity. As the NIPP is implemented, process measures will be deemphasized in favor of outcome measures. Examples include the reduction of risk measured by comparing 1 year of comparative analysis for a specific sector to another, and the overall risk mitigation achieved nationally by a particular CI/KR protection initiative.

3.6.1.2 Core Metrics and Sector-Specific Metrics

Quantitative indicators are used for two different groups of metrics to support national assessments: (1) core metrics, which apply to all sectors; and (2) sector-specific metrics, which are appropriate only for an individual sector.

Core Metrics are common across all sectors and represent a set of descriptive, process, and outcome data that enable measurement of progress in SSP implementation. Examples include the number of assets, systems, and networks with a potential for medium or high consequence, and the number of assets, systems, and networks with completed vulnerability analyses. Core metrics are basic measures that can be tracked across each sector to enable comparison and analysis between different types of CI/KR. Resources are allocated to those activities that best accomplish CI/KR risk-mitigation goals. Activities that do not advance these goals will be redesigned or eliminated over time.

Core metrics are consistent with the National Preparedness Goal and its supporting Universal Task List (UTL) and Target Capabilities List (TCL). DHS will specify an initial set of core metrics and work with SSAs and other security partners to refine them as experience in their use is gained over time.

Sector-Specific Metrics are tailored to the unique characteristics of each sector and are used to assist in monitoring progress within a specific sector. Sector-specific metrics and the means of monitoring progress against those metrics are

developed in a collaborative process that includes DHS, the SSAs, and other public and private sector security partners, as appropriate. For example, sector-specific metrics might include the percentage of shipments moving through a specific port that is subjected to detailed screening or improvements in the time required to obtain results from test samples.

3.6.2 Gathering Performance Information

DHS works with the SSAs and sector security partners to gather the information necessary to measure the level of performance associated with each set of core and sector-specific metrics. Given the inherent differences in CI/KR sectors, a one-size-fits-all approach to gathering this information is not appropriate. DHS also works with SSAs and sector security partners to determine the appropriate measurement approach to be included in the sector's SSP and to help ensure that security partners engaged with multiple sectors or in cross-sector matters are not subject to unnecessary redundancy or conflicting guidance in information collection. Information collected as part of this effort is protected as discussed in detail in chapter 4.

SSAs identify and, as appropriate, share or facilitate the sharing of best practices based on the effective use of metrics to improve program performance.

3.6.3 Assessing Performance and Reporting on Progress

HSPD-7 requires each SSA to provide the Secretary of Homeland Security with an annual report on their efforts to identify, prioritize, and coordinate the protection of CI/KR in their respective sectors. The report from each SSA will be sent to DHS annually. The reports are due no later than July 1 of each year.

The Sector CI/KR Annual Protection Reports provide the following information:

- Provide a common vehicle across all CI/KR sectors for communicating CI/KR protection performance and progress to security partners and other government entities;
- Establish a baseline of existing sector-specific CI/KR protection priorities, programs, and initiatives against which future improvements will be assessed;
- Identify sector priorities and out-year requirements with a focus on projected shortfalls in resources for sector-specific CI/KR protection and for protection of CI/KR within the sector that is deemed to be critical at the national level;

- Determine and explain how sector efforts support the national effort;
- Provide an overall progress report for the CI/KR sector and measure that progress against the CI/KR protection goals and objectives for that sector as described in the SSP;
- Provide feedback to DHS, the CI/KR sectors, and other government entities to provide the basis for the continuous improvement of the CI/KR protection program; and
- Help identify best practices from successful programs and share these within and among sectors.

SSAs work in close collaboration with sector security partners, the respective SCCs and the GCCs, and other organizations in developing this report. DHS works with SSAs to assess progress made toward goals in each sector based on these reports.

DHS compiles the sector reports into a national cross-sector report that describes overall progress toward CI/KR protection goals on a national basis and makes recommendations to the Executive Office of the President for prioritized resource allocation across the Federal Government to meet national CI/KR protection requirements. A more detailed discussion of the national resource allocation process for CI/KR protection is included in chapter 7.

In addition to these annual reports, SSAs regularly update their measurements of CI/KR status and protection levels to support DHS status tracking and comprehensive inventory update. By maintaining a regularly updated knowledge base, DHS is able to quickly compile real-time CI/KR status and protection posture to respond to changing circumstances as indicated by tactical intelligence assessments of terrorist threats or natural disaster damage assessments. This helps inform resource allocation decisions during incident response and other critical operations supporting the homeland security mission.

3.7 Using Metrics and Performance Measurement for Continuous Improvement

By using NIPP metrics to compare performance to goals, security partners adjust and adapt the Nation’s CI/KR protection approach to account for progress achieved, as well as for changes in the threat and other relevant environments. At the national level, NIPP metrics are used to focus Federal and security partner attention on areas of CI/KR protection that warrant additional resources or other changes. If a comparison of performance against goals using NIPP metrics reveals that there is insufficient progress (e.g., information-sharing mechanisms have not been established and risk assessments have not been conducted, or one or more sectors have a significant portion of their assets rated as high risk), DHS and its security partners will undertake actions to focus efforts on addressing those particular areas of concern.

Information gathered in support of the risk management framework process helps determine adjustments to specific CI/KR protection activities. For instance, as protective programs are implemented, the consequences and vulnerabilities associated with the asset, system, network, or function change. Accordingly, the national risk profile is reviewed routinely to help inform current and prospective allocation of resources in light of recently implemented protective actions or other factors, such as increased understanding of potential system-wide cascading consequences, new threat intelligence, etc.

In addition to quantitative measures, the NIPP provides mechanisms for qualitative feedback that can be applied to augment and improve the effectiveness and efficiency of public and private sector CI/KR protective programs. DHS works with security partners to identify and share lessons learned and best practices for all aspects of the risk management process. DHS also works with SSAs to share relevant input from security partners and other sources that can be used as part of the national effort to continuously improve CI/KR protection.

Figure 3-9: NIPP Risk Management Framework: Feedback Loop for Continuous Improvement of CI/KR Protection

