Homeland Security

Guidance and Template for Sector-Specific Plans

April 29, 2005

Deliberative Process/Pre-Decisional. Not Intended for Distribution.

This page intentionally blank

Table of Contents

This page intentionally blank

Preface

A fundamental objective of the National Critical Infrastructure Protection (CIP) Program is to identify and protect infrastructures deemed most "critical" in terms of their potential affects on national-level public health and safety, governance, economic and national security, and public confidence. The Department of Homeland Security (DHS) recognizes that such protection requires the cooperation and essential collaboration of federal departments and agencies, state, local, and tribal governments, and the private sector.

DHS issued initial *Guidance for Developing Sector-specific Plans (SSPs) as Input to the National Infrastructure Protection Plan (NIPP)* to Sector-Specific Agencies (SSAs) in April 2004 that was the basis for the draft SSPs that were delivered to DHS in September 2004. The content of these SSPs was evaluated against the *Guidance* and letters were issued to each SSA that detailed areas for improvement in the SSPs. The SSAs subsequently responded with their planned approach for addressing areas for improvement.

This template and guidance provides SSAs with additional information on what DHS expects that all SSPs should contain to ensure consistency and effective integration with the National CIP Program. This includes roles and responsibilities, new content, added emphasis on current SSP content, and updates to current content based on an evolution of the NIPP Risk Management Framework.

Roles and Responsibilities

In carrying out the responsibilities assigned in the Homeland Security Act of 2002 and further specified in HSPD-7, DHS, will:

- Coordinate the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States.
- Serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources.
  - *DHS leads the NIPP partnership at the Federal level.*
- Identify, prioritize, and coordinate the protection of critical infrastructure and key resources with an emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction.
  - *The NIPP Risk Management Framework implements this directive.*
- Establish uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors along with metrics and criteria for related programs and activities.
  - *DHS will establish, disseminate, and review the application of uniform guidelines for assessing and applying consequence, vulnerability, and threat information in NIPP risk assessment processes at the Sector and National levels.*

In carrying out the responsibilities assigned in HSPD-7, **SSAs** will:

- Identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies will work with State and local governments and private sector to accomplish this objective.
  - *This is the basis for SSA involvement across the NIPP Risk Management Framework (Set Security Goals, Identify Assets, (conduct) Risk Assessments, Normalize & Prioritize, Implement Protective Programs, etc.)*
- Collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector.
  - *SSAs are the lead Federal entity within their sector, leveraging other Federal interfaces and authorities that apply therein.*
- Conduct or facilitate vulnerability assessments of the sector.
  - *This is laid out in the Risk Assessment chevron of the NIPP Risk Management Framework.*
- Encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.
  - *Again, this is the basis for SSA involvement across the NIPP Risk Management Framework (Set Security Goals, Identify Assets, (conduct) Risk Assessments, Normalize & Prioritize, Implement Protective Programs, etc.)*

New SSP Content

- ***Sector Security Goals or Desired Security Posture –*** Describing what a sector should look like after risks are identified, weighed, and mitigated through successful implementation of the NIPP at all levels of engagement – whether by Federal, state, local, or private sector attention
- ***Sector Risk Assessment Processes –*** Describing how the sector will collaborate with DHS on the analytic criteria, tools, and risk analysis practices that support the sector's ability to identify and provide nationally usable information
- ***Sector Overall Risk Reduction Strategy –*** Laying out the types of protective measures that are most applicable to the sector across the protective spectrum (i.e., prevention, preparedness, mitigation, response, and recovery) and where they should be focused. This should be based on the sector's application of the revised NIPP risk management framework (the "chevrons") considering the physical, cyber, and human elements of assets
- ***Resource Identification –*** Indicating how the SSA will work with DHS, state, tribal, and local governments, and private sector owners and operators to identify available resources for protective measures (e.g., realigning budgets, federal grants, etc.)

SSP Content Added Emphasis

- ***Information Sharing –*** Identifying mechanisms available within the sector to communicate the NIPP message as well as mechanisms to enhance outreach to

owners, operators, local authorities, sector industry associations, and other interested parties to encourage their participation and contribution

- ***National CIP Manager and Sector-Specific Governance –*** Delineating the partnership between DHS, as the National CIP Manager, and the SSAs, particularly with respect to the completion of the Interim Period
- ***International Coordination –*** Discussing how sectors will coordinate with international organizations and foreign countries where there are assets located overseas or critical services and supplies originate from foreign countries
- ***Cyber Security –*** Expanding SSA asset identification, vulnerability assessment, risk assessment, and protective measures processes beyond physical assets to include cyber assets and cyber components of physical assets
- ***Sharing of Existing Sector Data –*** Specifying how SSAs will work with DHS to share existing data related to asset information, consequence of loss/attack, and vulnerabilities. This would include any prioritization schemes the sectors may have already developed and the associated descriptions of tools used and their results to allow DHS to analyze sector products for possible cross sector utilization

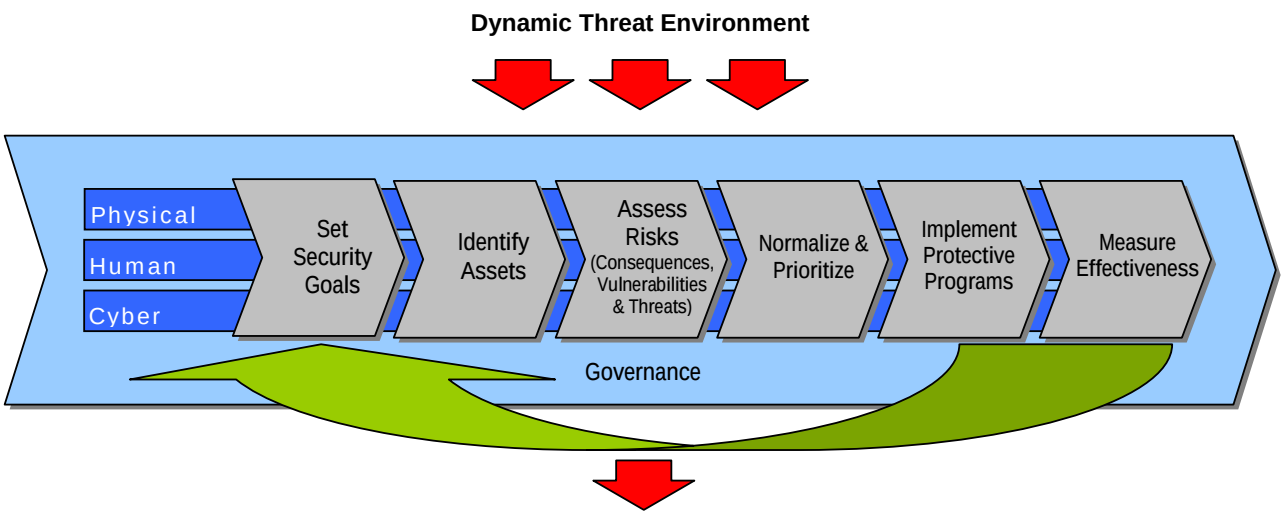
Updates to Current SSP Content

SSP content including Challenges, Initiatives, and Milestones should be updated to reflect current sector activities and status. In addition, the NIPP risk management framework has been updated since the publication of the Interim NIPP (Exhibit 1). The changes are summarized below:

- ***Chevron 1: Set Security Goals –*** These descriptions will serve as the objectives against which sector risks are compared, resulting in specific protective strategies and initiatives to address any shortfalls. The SSA should also identify areas of interaction with other sectors and work closely with DHS and the other concerned sectors for a unified cross-sector strategy under the leadership of DHS. Risk should be assessed against these security goals and protective programs designed to correct shortfalls. Over time, the NIPP will raise the Nation's security posture as expressed in these goals across the 17 critical infrastructure/key resource (CI/KR) sectors
- ***Chevron 2: Identify Assets –*** The text *"Identify Critical Infrastructure"* was replaced with **Identify Assets** to reflect the need for SSAs to screen and nominate assets with significant consequences for the purpose of a more detailed assessment of risk to be conducted in Chevron 3. Only after an asset has been thoroughly assessed will it be possible to determine whether an asset is indeed critical to national risk
- ***Chevron 3: Assess Risks –*** The text was changed from *"Identify and Assess Vulnerabilities"* to **Assess Risks (Consequences, Vulnerabilities, and Threats)** to better reflect the focus on the importance of risk (which includes assessment of consequences, vulnerabilities, and threats) as the driver for prioritization, protective actions, and measures of effectiveness
- ***Chevron 4: Normalize and Prioritize –*** The word *"Analyze"* was deleted to reflect that analysis naturally occurs in all of the risk management framework chevrons. **Prioritizing** CI/KR is based on normalization of the risk data (i.e., threats, vulnerability, and consequences) across sectors to determine national risk

- ***Chevron 5: Implement Protective Programs –*** There were no changes to the text in this chevron pertaining to developing consistent, sustainable, measurable, and effective **programs to protect** CI/KR and implementing those programs.
- ***Chevron 6: Measure Effectiveness –*** The text *"Through Performance Metrics"* was deleted as this is implied by the text **Measure Effectiveness**
- ***Governance (Underlying all Chevrons) –*** Because the activities of the framework require significant and, in some cases, unprecedented coordination among all stakeholders, we have added **Governance** as a key activity supporting every step of the risk management process to ensure effective management and resolution of issues that arise

Exhibit 1: NIPP Risk Management Framework



Sector-Specific Plan Outline

Chapter 1: Document Sector Background & Engagement

A. Sector Profile
B. Review of Authorities
C. Mapping Relationships
D. Coordinating Structures
E. Information Sharing Mechanisms

Chapter 2: Establish Sector Security Goals

A. Process to Establish Sector Security Goals
B. Sector Security Goals and Objectives

Chapter 3: Identify Sector Assets

A. Process to Identify Sector Assets
B. Updating Asset Data
C. Protecting Asset Data

Chapter 4: Assess Sector Risks

A. Process to Assess Sector Risks

Chapter 5: Normalize & Prioritize

A. Process to Normalize and Prioritize Sector Assets

Chapter 6: Implement Protective Programs

A. Process to Implement Protective Programs

Chapter 7: Measure Progress

A. Process to Develop Sector-Specific Metrics
B. Reporting Responsibilities

Chapter 8: Plan CIP Research and Development

A. Sector Technology Requirements
B. Current R&D Initiatives
C. Gaps
D. Candidate R&D Initiative

Chapter 1: Document Sector Background & Engagement

Purpose: In this chapter, SSAs will characterize their sector, describe the context in which the SSA engages with the stakeholders, and identify authorities and regulations relevant to protective activities. This section of the SSP will provide a "snapshot" of the sector and describe how involved the various stakeholders are in conducting protective activities.

Note: DHS is particularly interested in the identification of any structural, regulatory, or other background characteristics of the sector that should be considered in risk management decisions at all levels (e.g., Federal, state, local, private) of the NIPP partnership.

Benefits: This information will ensure that the readers of a SSP understand the nature and complexity of the sector and the current relationships among stakeholders. DHS will use this information to understand how the SSA views its sector responsibilities, to obtain information on the key stakeholders in the sector and how they relate to each other, and to determine legal authorities for implementing the program.

A. Sector Profile

Sector profiles should be updated to reflect further definition and understanding of the sector as a result of sector engagement activities (e.g., interaction with owners and operators, GCCs/SCCs, trade associations).

SSPs should include the following information in this section:

- Concise definition of sector boundaries and characteristics of assets and ensure that any potential gaps, as well as any overlaps in scope between sectors, are identified and addressed
- Characterization of the sector assets including, where appropriate, sub-categorizations or classes of assets, particularly if the sector includes obviously distinct types of operations, businesses, facilities, etc. For example, at the highest level, the transportation sector will be divided into transportation modes (e.g., air, rail, highway, maritime, etc.)
- Description of the entities that own or operate the various assets or classes of assets (e.g., owners who are private industry versus municipalities)

B. Review of Authorities

Sector governing authorities should be updated to reflect laws, rules, regulations, orders, etc., applicable to the protection of assets within the sector. The SSP should also identify the gaps in authority that could hinder the CIP process.

This should include any authorities pertinent to:

- Collection of asset-specific information (e.g., can a permitting authority be used to collect pertinent information relevant to the structure or operation of a particular facility?)
- Information sharing and protection
- Conducting vulnerability and risk assessments (e.g., for some sectors, vulnerability and risk assessments are already required under other statutes, such as the Bioterrorism Act)
- Identifying protective strategies
- Implementing protective programs

C. Mapping Relationships

The effective engagement of sector stakeholders by SSAs must utilize relationships and activities that are proven to be effective and also employ new approaches to streamline and expedite action. The status of the SSA's current relationships within the sector will be useful in identifying successful efforts, in recognizing the complexity and diversity of sectors that require active subcomponents, and in targeting areas where further outreach is desired and assistance from DHS may be helpful.

SSPs should contain a description of sector relationships with stakeholders as discussed in the following sections.

- ***Private Sector Owners/Operators and Organizations*** – Identify existing relationships as well as general expectations for how these stakeholders will support the development and implementation of the SSP
- ***Other Federal Departments and Agencies*** – Identify the departments and agencies that will provide a supporting role. Describe the SSA's current relationship with those agencies as well as expectations for their roles and responsibilities in developing and implementing the SSP
- ***State and Local Agencies*** – Describe relationships with state and local agencies and expectations for their roles in supporting the development and implementation of the SSP
- ***International Organizations and Foreign Countries*** – Describe relationships with any international organizations and foreign countries pertaining to cross-border assets and supply of critical materials or components

D. Coordinating Structures

SSPs should include the following information in this section:

- All NIPP-related coordinating mechanisms and structures, whether public or private
- Relationships of coordinating mechanisms and structures
- Basic concept of operations

Coordinating structures and mechanisms should be discussed for the following stakeholders at a minimum:

- ***NIPP Coordination Councils –*** Composition of sector GCCs, SCCs, frequency of meetings, and progress in establishing these councils as sector management for the sector-specific risk reduction planning and activities
- ***State, Local, Tribal Government Entities*** – Role in sector operations, safety and security, planning, and risk reduction activities and level of integration of these entities in the sector
- ***International –*** To accurately characterize their sector, SSAs must account for U.S. assets located abroad. The potential interconnectedness of U.S. CI/KR with foreign countries' CI/KR also requires that SSAs consider interdependencies of U.S.-owned infrastructure with foreign infrastructure. The level of detail required to address the international component in each SSP will depend upon each sector's unique characteristics and composition.

E. Information Sharing Mechanisms

This section of the SSP should identify preferred information sharing mechanisms for the sector from those available within public and private sector channels.

Include examples of information sharing and communication mechanisms developed by DHS to ensure that protection programs are operationally coordinated, and that threat and other security-related information is shared with appropriate stakeholders.

Chapter 2: Establish Sector Security Goals

Purpose: The purpose of this part of the Plan is for the SSA to develop Sector Security Goals to provide clear direction for the sector's CIP efforts.

Benefit: The entire risk management framework is tied to the Sector Security Goals. The sector goals are driven by a desired reduction in risk, which is achieved through the application of specific protective strategies and initiatives.

A. Process to Establish Sector Security Goals

Effective critical infrastructure protection partnerships must be built on a common vision of "steady states" for the sector. Achieving a secure, protected, and resilient infrastructure implies a set of sector-specific security goals (i.e., specific outcomes, conditions, end points, or performance targets) that collectively represent a successful security posture. Each sector has distinct assets, operational processes, business environments, and risk management approaches that determine the security goals the sector will pursue. Such goals reflect the overall risk management outcomes that owners/operators and government leaders seek to produce for their sectors. These goals should consider the desired future status of physical and cyber security as well as the many dimensions of the protective spectrum. We anticipate such security goals will vary considerably across sectors, and probably even within sectors, depending on the internal structure and composition of a specific industry component.

The SSP should outline the engagement strategies used to develop security goals. During the Interim Period and beyond, SSAs and DHS must work closely with public and private sector stakeholders to reach consensus on a sector's overall security goals. DHS will provide assistance to SSAs in the form of facilitated Technical Assistance Sessions to develop their sector security goals based on a cross-sector template.

B. Sector Security Goals and Objectives

The SSPs should provide the outcome of the process in terms of the agreed upon sector security goals and any associated objectives. It should also include the process the SSA plans to use to evaluate the sector security posture as the sector changes.

Chapter 3: Identify Sector Assets

Purpose: The purpose of this part of the Plan is for the SSA to explain the process it will use to gather information on those sector assets that *could potentially be critical* (i.e., those that, if damaged would result in significant consequences – impacts on national economic security; loss of life; national public health, safety, psychology; or some combination of these).

Benefit: This data gathering and analysis will provide the SSA and DHS with a comprehensive inventory of critical assets, which can then be further analyzed with respect to vulnerabilities and protective actions.

A. Process to Identify Sector Assets

SSPs must address the methodology for identifying and maintaining current data on CI/KR. The starting point for this is a threshold analysis which considers that not every individual component of the sector systems (e.g., all telephone poles or all transformers) is pertinent to this effort. Asset identification should focus on those assets or systems that are large enough to be considered targets for attack and that may potentially be candidates for protective actions.

Asset selection may vary greatly depending on the unique structure of the sector. In some cases it may be helpful to identify asset classes or categories, rather than discrete assets. Examples include aircraft or vessels of a certain size or type, types of financial institutions, or groups of individuals, such as maintenance personnel. Such categories may support the identification of assets that are more people-oriented or intangible in nature (e.g., the airspace in a region). In some cases, more intangible assets can be linked with one or more physical or cyber assets in the same system (e.g., regional airspace with the regional control system).

Deciding that an asset meets the criteria established for national risk reduction analysis does not yet equate to deciding its criticality, which is analyzed in the next chevron. DHS will work with SSAs to develop an approach to asset identification that addresses sector-specific issues while remaining consistent with the overall NIPP cross-sector analytic approach.

This SSP chapter should document current or proposed approaches to identify sector assets, data sources of such information, and plans to validate such inputs, as follows:

1) Defining Asset Data Parameters

As a first step in identifying assets across the sector, the SSA must first define the specific information that it will collect about each asset. In identifying assets, SSAs must ensure that they take a comprehensive, integrated view of the asset to include all of its characteristics and dependencies for it to function. Many assets are dependent on multiple elements and systems to maintain functionality (e.g., people, physical, cyber, etc.). SSPs should include a discussion on:

- How the sector defines the universe of assets, including sub-sectors. Note: these definitions should reflect the jointly developed sector taxonomy and include sufficient information to understand the functioning of an asset and to conduct consequence of loss analysis in the areas of concern
- The threshold level to be used in identifying assets of consequence requiring further analysis, and why this level is appropriate

2) Collecting Asset Data

The next step is to identify and describe how the SSA will collect or obtain access to this information, currently and in the future (as the information will constantly change). At a minimum, the description of this data collection process must include:

- What information on sector and cross-sector assets is currently available?

- How and when will existing information be formatted, linked, and provided to DHS for inclusion in the National Asset Database (NADB)?
- What processes will be utilized to gather the information required to inventory a sector's infrastructure beyond the SSA's current holdings?
- Where will asset information collected be housed other than in the NADB?
- What asset information protection mechanisms are in place or planned?
- How and how often will the data for the sector's assets be provided to DHS for inclusion in the NADB?

3) Verifying Asset Data

Once the asset data have been received by the SSA, they must be verified. In this section of the Plan, the SSA will describe the quality control process for ensuring that information collected is reliable. The process for verifying data for assets must include the following:

- How the SSA will verify asset information
- Protocol for reviewing data (e.g., sample size, criteria, frequency)
- Steps to address incomplete and/or inaccurate data
- Follow-up activities required based on the infrastructure's significance (e.g., onsite meetings, validation of owner/operator procedures, etc.)

B. Updating Asset Data

Asset data from the sector must be routinely updated and made available so that the SSA and DHS will be able to leverage the most up-to-date data when making decisions concerning national protection strategies. This section of the plan must describe the SSA's process for ensuring access to continuously updated asset data for the sector. The process should include the following:

- Frequency of updates (e.g., as changes occur and/or on a routine basis)
- How updated information will be provided
- Considerations for reevaluation of the sector inventory itself
- SSA division/office that will be responsible for obtaining the data
- How the SSA will notify DHS of data updates
- How asset information will be maintained—where and by whom?
- What additional information protection mechanisms are needed for the NADB and SSA databases to facilitate information sharing?

C. Protecting Asset Data

Sector asset data may qualify for one or more exemptions from public disclosure under the Freedom of Information Act (FOIA). SSAs should consult with the FOIA Officers and/or Offices of General Counsel of their respective agencies to obtain specific guidance on the possible protections from public disclosure by one of the exemptions or special exclusions.

The Protected Critical Infrastructure Information (PCII) Interim Rule does not afford protection to voluntarily submitted critical infrastructure information unless it is submitted directly to DHS. Refer to the PCII Program web site at www.dhs.gov/pcii for specific details on how to properly submit the information to the PCII Program Office at DHS. The process of protecting asset data should include the following:

- Security classification of the data
- What asset information protection mechanisms are in place or planned?

Chapter 4: Assess Risks

Note: Until the Interim NIPP and its risk management framework are revised and issued, SSPs will not be expected to address all of the items in this section.

Purpose: The purpose of this part of the Plan is twofold. First, it seeks to have each SSA describe its current approaches for assessing risks to assets in its sector and to describe how this information will be provided to and/or shared with DHS in the near term. Second, the Plan also solicits input on how assessment methods unique to the sector can be reviewed and, if necessary, modified to allow both SSAs and DHS to achieve compatibility with assessment methods and data from other sectors. Where standardization is not possible or desirable, DHS will work with each sector to normalize its existing vulnerability and risk assessment results.

The purpose of both parts of this section of the SSP is to promote standardization of data through the greater use of common assessment methods and measurements for risk in order to provide a level playing field for the prioritization and distribution of resources from the national and sector agencies.

At the end of the sector risk assessment process, DHS expects each SSA to produce an ordered set of sector assets and accompanying risk assessment data according to the sector view of their relative risk. Over time, the perspective and corresponding measurements of the relative levels of risk should increasingly be expressed using a common national risk scale. Regardless of how such measurements of risk are expressed, this data will be one of several sector inputs needed to produce assessments of national risk in the Normalize & Prioritize chevron.

Benefits: The consistent evaluation of consequences, vulnerabilities, and threats will allow the SSA and asset owner/operators to understand where protective strategies are most needed due to the potential for significant consequences stemming from a high risk event. DHS will use this information to select those assets across all sectors that warrant the most attention in terms of protective strategies as well as to help determine research needs and priorities.

A. Process to Assess Risk

Risk assessment combines the evaluation of potential consequences, threats, and vulnerabilities in a holistic manner. When provided to DHS annually, this information will be used to provide standardized cross-sector comparisons, interdependency analysis, resource allocation decisions, and risk assessments using current intelligence of evolving threat streams, which is in the third chevron in the NIPP risk management framework.

To ensure that the vulnerability and risk assessment methodologies used or proposed for use in the sector will result in data that supports comparison within and across sectors, this section of the SSP should detail the methodologies SSAs will use and how such methodologies conform to DHS guidelines. Where existing assessment tools do not conform to DHS guidelines, sectors can engage their GCC to begin working with DHS to consolidate and normalize their risk assessment results. In particular, the SSPs must contain a discussion of each sector's strategy to help coordinate and implement the following initiatives:

- ***Common Risk Management Vocabulary –*** As with any profession, a set of commonly accepted and consistently used definitions for the key professional terms is necessary to have productive discussion among its membership. DHS intends to facilitate the coordination of a commonly accepted set of definitions for security risk analysis to improve the ability for the SSAs, state, tribal, and local governments, and sector owners/operators to communicate effectively.
- ***Common Threat Scenarios –*** To facilitate providing threat data to the sectors for their use in risk assessment, DHS will provide the sectors with appropriate threat scenarios (with corresponding threat rankings) for their use in the risk assessment process. By standardizing this input into the risk assessment process, DHS can provide sectors a more useful and efficient threat assessment.
- ***Common Scales –*** The ability to make valid inter-sector and intra-sector comparisons is dependent on the use of a consistent unit of measurement for consequences and corresponding scale for consequences, vulnerabilities, and threats. DHS expects to work with sectors to develop a common national scale that all sectors can use to make their assessment results comparable at the national level and more easily understood outside of each sector.
- ***Generally Accepted Risk Assessment Practices –*** The ability to assess and measure risks is dependent on consistently applied principles and practices. This allows self-assessment teams to apply their reviews in an analytically rigorous way consistent with the assumptions used by others. Working with all of the sectors, DHS will develop a consistent set of guidance documentation to allow the assessment of individual assets to be conducted in accordance with widely-accepted practices across all sectors.

To assist in integrating these DHS initiatives into the national risk management program, the SSP must describe how the SSA will undertake the following:

- ***Asset Selection for Further Analysis –*** Consequence analysis to determine which assets – physical, cyber, and human aspects – pose enough concern to warrant further analysis (i.e. which assets result in significant consequences).
- ***Identify and Collect Current Vulnerability and Risk Assessment Data –*** SSAs can collect existing asset, consequence, vulnerability, and risk assessment data within their sector and coordinate with DHS to ensure this information is compatible with other assessment data in the national risk management framework.
- ***Identify and Assess Sector-Specific Tools –*** SSAs should identify tools used within the sector and then work with DHS to determine whether these tools can be modified to result in data that is compatible with the national risk management program.
- ***Build a Risk Analysis Capability –*** SSAs should describe how they will identify specific personnel who can be trained in the sector's accepted vulnerability and risk assessment methodologies.
- ***Encourage Stakeholder Implementation –*** SSAs should identify how they plan to encourage sector stakeholders to embrace the process and conduct assessments at their own facilities. This can be done, in part, by providing sector stakeholders with the common set of risk assessment tools, along with guidance that emphasizes the importance of consistent application. SSAs can then solicit feedback from private sector participants in these assessments to gather lessons learned and best practices.
- ***Assist in Interdependency Analysis –*** SSAs are aware of unique systems, capabilities, and processes carried out within their sector and they should use that knowledge to inform the interdependency analysis process. Because of the vast

differences between assets within and across sectors, SSAs should identify how they will work with DHS to ensure that the interdependency analysis methodology is informed by all the necessary information and that all identified linkages are communicated to the other affected SSAs so that the appropriate planning can occur.

Chapter 5: Normalize & Prioritize

Note: Until the Interim NIPP and its risk management framework are revised and issued, SSPs will not be expected to address all of the items in this section.

Purpose: This chevron is primarily DHS's responsibility, although it may also be performed to a lesser degree in the sectors themselves. It is intended to incorporate a validated assessment of component risk factors (threat, vulnerabilities, and consequence) with their known inter- and intra-sector dependencies to produce an ordered assessment of those assets representing national risk.

Benefits: A systematic and consistent way of prioritizing assets offers transparency and increases the defensibility of the decisions that are made about resource allocation. It also reduces the focus on individual companies or assets and helps to determine what is of national importance in terms of potential impact. The results will serve to provide a level playing field for DHS and the sectors in their prioritization of protective actions conducted with Federal resources.

A. Process to Normalize and Prioritize Sector Assets

Although from a national perspective, creating greater uniformity in assessment results within and across sectors is a desired goal of the NIPP framework, this outcome will take significant collaboration between DHS and SSAs and between SSAs and their sectors. In the near team this will not always be achievable. Where standardization of the resulting risk data is not immediately achievable, DHS intends to coordinate with SSAs to "normalize" or translate their risk assessment results in such a manner that they can be compared against other sectors and other methodologies for the purposes of prioritizing assets and making resource decisions.

SSAs should solicit from their sectors vulnerability and risk assessment methodology information for the purpose of determining how such methods determine any qualitative and quantitative ratings for consequences, vulnerabilities, and threats. In their SSPs, SSAs will identify how such approaches are conducted and their assessment of how the data resulting from the different approaches can be normalized.

The normalization step provides an additional opportunity for DHS review and incorporation of all applicable intelligence threat information, regardless of classification, sensitivity, and recency. It also allows DHS to integrate the results of other sector assessments where cross-sector interdependencies significantly impact the overall consequences and in turn, increase risk beyond what the sector can calculate with its own data.

In the SSPs, SSAs will identify how they plan to coordinate with their asset owners and operators to identify other infrastructures upon which their assets rely and also the other infrastructures and assets they believe rely on them.

Finally, the prioritization of all assets is conducted after assessment results are normalized and validated by DHS, interdependencies are factored into the analysis, and any additional or recent threat information are incorporated.

Chapter 6: Implementing Protective Programs

Purpose: In this part of the Plan, the SSA will explain how it will work with sector stakeholders to develop one or more sector-specific programs to protect its high-risk assets.

SSAs and other sector stakeholders are encouraged to take protective actions on the highest priority items identified within their sectors, in close coordination with DHS exercising its national CIP risk reduction responsibilities.

Benefits: Protective programs guide asset owners/operators on the most effective strategies given the general classes of threats that are applicable to that sector and the vulnerabilities common to the assets in the sector.

A. Process to Implement Protective Programs

Within and across sectors, protective actions are implemented by a range of stakeholders, including DHS, SSAs, state and local authorities, and owners/operators. A protective program is a coordinated plan of action to prevent, deter, and mitigate terrorist attacks on critical assets, as well as to respond to and recover from such attacks in a manner that limits the consequences and value of such attacks. Each sector needs a tailored strategy and programs to best protect the critical assets within the sector.

This section of the SSP should contain a discussion of the current or proposed processes for developing protective programs to implement their selected strategies. In particular, the SSP should identify:

- ***Security Strategies***
  - The most suitable balance of prevention, protection, response, and recovery by sector, sub-sector, or asset class
  - How these influence guidelines or minimum standards for protective actions
- ***Decision-Making Processes***
  - Processes for assessing anticipated costs of protective actions, including purchasing data sources
  - Processes for balancing costs against the risks for particular assets
  - Role of stakeholders in carrying out these analyses
- ***Protective Program Implementation***
  - What protective actions are appropriate for the sector and why (tie into goals)
  - How sector-specific protective actions are coordinated with actions implemented by DHS
  - Who conducts protective programs and under what circumstances
  - How protective actions are tracked
  - Use of best practices and information sharing in encouraging stakeholder implementation

- Roles and responsibilities of sector stakeholders
- How critical information generated from plan implementation, particularly the information on which assets appear to pose the highest risk, will be considered
- How stakeholders will share best practices for long-term protective programs, including overcoming implementation challenges
- How often and by which entity the protective programs will be updated and refined

Particular attention should be paid in the process to identifying the appropriate roles of the sector stakeholders. The role of some stakeholders (e.g., Federal agency) may be to create the atmosphere or encourage the implementation of protective programs. Other stakeholders will ultimately take actions for implementing the protective programs. The roles should reflect existing authorities (e.g., regulatory) and relationships of the sector stakeholders.

The protective program should, at a minimum, ensure that it covers those assets that appear to have the highest risk. General approaches for protecting assets include:

- ***Prevent or Delay an Incident –*** Enhancing police presence, restricting access, fencing, structural integrity, vehicle checkpoints, and cyber protection features such as additional access controls. Within the sector, such measures are generally taken by the asset owners/operators and may vary by threat level.
- ***Detect a Potential Incident –*** Intrusion detection systems, monitoring, operation alarms, and employee security awareness programs. These actions are also taken at the asset level and are generally permanent changes.
- ***Mitigate or Respond to an Incident –*** Adequate response plans can mitigate impacts and potentially enable the sector asset to resume operations sooner. Such plans may involve multiple stakeholders within the sector, including state and local agencies.
- ***Recover from an Incident –*** Continuity of operations plans. These plans may be asset-specific or it may be developed for a set of assets.

Both mitigation and recovery can benefit from additional redundancy at either an asset or sub-sector level.

Protective programs should separate actions for tactical response (e.g., ISAC threat information needing action within hours or days) versus more long-term strategic response. DHS will play the lead role in developing tactical measures for the most critical assets in response to specific threats. The sector stakeholders will address more long-term strategies (e.g., redundancy) as well as tactical responses for other assets and for those measures within the control of the asset owner/operator.

Chapter 7: Measuring Progress

Purpose: This part of the Plan explains how SSAs will design and implement performance metrics for implementation of SSPs.

Benefits: Since performance metrics are directly related to sector security goals identified in Chapter 1, an effective measurement system serves to clarify these goals in the planning process. Measurement quantifies the benefits achieved by CIP activities and supports feedback to improve program activities and better allocate resources. While tracking program performance and progress is the last step in the CIP Program implementation process, performance metrics will be used to constantly improve the alignment of protective programs to the dynamic threat environment, and to drive higher awareness of the threat

environment among critical infrastructure owners/operators. This process will provide the information necessary to assist senior officials in making informed decisions about protective actions and national risk management. In addition, metrics will measure program accomplishments and drive continuous improvement of CIP activities.

A. Process to Develop Sector-Specific Metrics

Each SSP should include development of sector-specific metrics. The SSA should define its CIP goals and provide a short, focused, and manageable list of process and outcome metrics, organized by asset class if appropriate. These goals and metrics will differ by sector, depending upon the maturity of the existing CIP program and specific characteristics of sector assets and operations.

SSAs should strive for outcome metrics. The principal intended outcome of sector CIP programs is the reduction of risk through reducing vulnerability, potential consequences, or the likelihood of attacks. Sectors with mature risk assessment methods should define risk-based outcome measures. For example, the use of risk assessment results to measure reductions of risk due to the targeted application of protective measures.

Other intended outcomes could include:

- Reducing the cost of protective actions (e.g., lower-cost baggage screening)
- Maximizing the operating efficiency of assets with protective actions in place (e.g., lower wait times a airport checkpoints)
- Increasing public confidence in the security of sector activities (e.g., traveler confidence)

B. Reporting Responsibilities

HSPD-7 calls for sectors to report annually to the Secretary of Homeland Security on progress. For this Interim Period, SSAs will be asked to report back to DHS on each of the three components by September 30, 2005.

Chapter 8: Planning CIP Research and Development

Purpose: This part of the Plan explains how research and development (R&D) considerations will be incorporated into the NIPP. It explains the roles of SSAs, DHS's Information Analysis and Infrastructure Protection Directorate (IAIP), DHS's Science and Technology Directorate (S&T), and the Office of Science and Technology Policy (OSTP) in developing sector-specific summaries of R&D plans.

While not specifically outlined in the CIP risk management process as a chevron, one of the implementation requirements of HSPD-7 is the development of an annual R&D plan on CI/KR protection. The SSP R&D chapter should describe how the sector will strengthen the linkage between sector-specific and national R&D planning efforts.

Each SSA should identify the person responsible for R&D planning for their sector, and that person, or their representative, should participate in the ongoing DHS S&T/OSTP planning process.

Benefits: Many CIP challenges call for science and technology solutions. The Federal CIP R&D Plan will inventory current Federal R&D initiatives that have potential CIP applications, indicate technology requirements, identify gaps, and indicate planned R&D initiatives. It will also identify issues that may benefit from the initiatives of industry or academia.

A. Sector Technology Requirements

In this section, SSAs should provide a description of the processes they will use to identify sector technology requirements and communicate them to S&T/OSTP for inclusion in the Federal CIP R&D Plan on an annual basis. The processes should ensure that requirements will be identified by theme. The information required from SSAs will include a summary of technology requirements in their SSP chapters which highlight requirements without the more detailed explanations included in the Federal CIP R&D Plan.

B. Current R&D Initiatives

SSAs should describe the process they will follow to annually solicit a listing of current Federal R&D initiatives from S&T/OSTP that have potential to meet their sector's CIP challenges. In this section of the Plan, the SSAs should then describe how they will analyze this listing with the help of S&T and sector stakeholders and how they will indicate which initiatives have the greatest potential for positive impact. The process should ensure that impacts align with the performance measures as described in Chapter 7 of the SSP.

C. Gaps

The Plan should address how SSAs will solicit an analysis of the gaps between the sector's technology needs and current R&D initiatives from S&T/OSTP. S&T will determine these gaps as opposed to each sector doing so independently, because gaps will often be shared by multiple sectors. In this section, SSAs will describe the process by which they will summarize the most important gaps for their sector, as identified by S&T. The roles of different parties within the sector in making this determination should be described.

D. Candidate R&D Initiatives

The Plan should also describe how SSAs will solicit descriptions of candidate R&D initiatives from S&T/OSTP to fill gaps. S&T can view cross-sector technology gaps holistically, and can identify opportunities for an initiative sponsored by one sector to support other sectors. This will focus R&D investments on the highest national CIP priorities and identify multiple-use technology solutions. In this section, SSAs will summarize the process by which they will determine which candidate R&D initiatives are most relevant for their sectors, as identified by S&T, and how these will be summarized.

This Page Intentionally Blank

Next Steps

As the Interim Period progresses, DHS and the SSAs will work together, along with other Federal departments and agencies; state, local, and tribal entities; and the private sector to continue refining stakeholder roles and responsibilities. This will require frequent contact between the SSAs and DHS as key elements of the SSPs are developed. Particular attention should be given to processes such as stakeholder engagement, adoption of the risk management framework including the risk analysis process, and implementation of metrics within each sector. This will ensure that DHS and the SSAs are working in concert to align sector- and process-building activities across all 17 CI/KR sectors.

Technical Assistance Sessions

To assist with the implementation of this Guidance for SSPs, DHS will host a series of Technical Assistance Sessions. These sessions will feature speakers from DHS, as well as other CIP experts, and will focus on topics that are relevant to the Interim Period. All sessions will be held on the Concourse Level at 1725 EYE Street, NW, Washington, DC 20006. The schedule of Technical Assistance Sessions is as follows:

Session 1, *Sector Security Goals and Outreach*
Wednesday, May 4, 2005
1:00-3:00

Session 2, *Asset Identification*
Thursday, May 12, 2005
1:00-3:00

Session 3, Risk: *Threat-Based Assumption*
Friday, May 20, 2005
1:00-3:00

Session 4, *Risk Assessment*
Thursday, May 26, 2005
1:00-3:00

Session 5, *Cyber*
Thursday, June 2, 2005
9:00-4:00 (***all day***)

Session 6, *Metrics and Reporting*
Wednesday, June 15, 2005
1:00-3:00

Session 7, *Resource Requirements*
Thursday, June 30, 2005
1:00-3:00

Session 8, *R&D*
Thursday, July 14, 2005
1:00-3:00

Session 9, *TBD*
Thursday, July 28, 2005
1:00-3:00

Session 10, *TBD*
Thursday, August 11, 2005
1:00-3:00

Note that after the Technical Assistance Sessions, DHS may coordinate with the SSAs to schedule individual sector meetings to discuss the session's topic area in greater detail as needed. Sessions are scheduled to run until 3pm, but discussion can continue as needed until 5pm.

Key Interim Period SSP Milestones