National Protection and Programs Directorate

Office of Infrastructure Protection Strategic Plan: 2012–2016

August 2012

Homeland Security

Collaborate

Our Nation’s critical infrastructure—both physical and cyber—is crucial to the functioning of the American economy and our way of life. Critical infrastructure provides the means and mechanisms by which critical services are delivered to the American people; the avenues that enable people, goods, capital, and information to move across the country; and the engine that underpins the Nation’s defense, manufacturing of goods, production of energy, and our overall system of commerce. Our critical infrastructure is increasingly connected and interdependent and protecting it and enhancing its resilience is an economic and national security imperative.

Although infrastructure protection and resilience is a whole-of-Nation activity, the Office of Infrastructure Protection (IP) is at the center of this effort. We support the Secretary of Homeland Security’s national leadership role by working with critical infrastructure owners and operators to develop and monitor risk management approaches and other preparedness and resilience measures that enhance security. We do this in many ways, including analyzing risks and sharing information to manage those risks, conducting vulnerability and resilience assessments, developing standards and best practices, supporting and informing preparedness and incident management activities, and ensuring compliance with regulatory frameworks. Our goal is to incentivize and influence action by our partners that will reduce risk and enhance preparedness for all hazards.

Given the nature of our mission, we must work in close collaboration with all levels of the public, private, and non-profit sectors. We must strive as an organization to be a trusted source of information and knowledge and a responsive partner, and we must protect the critical infrastructure and personal information with which we are entrusted. We must also challenge ourselves and our community to prioritize those efforts that are most likely to deliver cost-effective value by enhancing the security and resilience of the country’s most vital assets, systems, and networks.

We cannot be complacent in our mission. Events of the 21st century have already shown that we live in a dynamic and global risk environment, defined by new and evolving threats and challenges to the Nation’s infrastructure. Acts of terrorism remain persistent threats, with our adversaries looking for ways to exploit new technologies to bring harm to the United States and its allies, while extreme weather events are exacerbated by their potential impact to critical infrastructure, much of which is aging, overtaxed, or at risk of failure in extreme conditions. In addition, attacks in cyber space have demonstrated that actions taken via a computer can manifest through consequences that include potentially degrading the functioning of our physical and cyber infrastructure.

IP needs to be prepared to adapt to an evolving risk environment. Our mission demands a risk-informed and learning organization with systems that quickly collect and interpret information to allow us to work with partners to develop and implement innovative solutions. This Strategic Plan is designed to help us along that path. It defines our goals and objectives and reiterates our commitment to promote organizational excellence and empower our employees by making IP a world-class organization that is dedicated to employee growth and opportunity. I invite all of you to read it and, while doing so, to reflect on your role in helping make the Nation more secure.

Caitlin A. Durkovich
Assistant Secretary
Office of Infrastructure Protection

1. Introduction

Our Nation's critical infrastructure is essential to the economy, security, and sustainment of the American way of life. From the provision of essential goods and services—including energy, communications, food, and water—to the facilitation of essential commerce such as our transportation networks and critical manufacturing base, the owners and operators of America's critical infrastructure enable the daily activities of our country. Securing our physical and cyber infrastructure, helping to modernize it, and making it more resilient is a crucial part of our homeland security effort. We must continue to prioritize a strategic approach to accomplishing that mission.

A major element of accomplishing that mission is the Department of Homeland Security's National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP), which leads the coordinated national effort to manage risks to our Nation's critical infrastructure. IP acts on behalf of the Secretary of Homeland Security, helping execute the national critical infrastructure protection responsibilities set forth in Homeland Security Presidential Directive 7 (HSPD-7). The vast majority of our Nation's critical infrastructure is owned and operated by the private sector, and IP's strategy is based largely on building partnerships, planning for preparedness, and sharing information and tools to ensure the availability, security, and resilience of the Nation's critical infrastructure.

IP is an internationally recognized critical infrastructure protection and resilience organization. We lead and coordinate national programs and policies and have established strong partnerships across government and the private sector. We conduct and facilitate vulnerability and consequence assessments to help critical infrastructure owners and operators and State, local, tribal, and territorial partners understand and address risks. We provide information on emerging threats and hazards so that appropriate actions can be taken. We offer tools and training to our partners to help them manage the risks to their assets, systems, and networks.

Our efforts also increase awareness within the critical infrastructure community about the need to prepare for all hazards. We conduct exercises to ensure that government and private sector partners can work together effectively before, during, and after an incident. We gather and analyze data to improve planning and response efforts and to support all our programs and activities. In addition, IP is the Sector-Specific Agency (SSA) leading the focused protection and resilience efforts for six of the critical infrastructure sectors—Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, and Nuclear. IP also has the responsibility for chemical security regulatory programs: the Chemical Facility Anti-Terrorism Standards and ammonium nitrate programs. IP's organization supports and integrates these diverse activities; please see Appendix A for an overview of the organization and the missions of its divisions.

This 2012 – 2016 Strategic Plan builds on IP's history of promoting critical infrastructure risk management and provides the IP workforce with a common mission and vision that guides the work we do every day in protecting and enhancing the resilience of the Nation's critical infrastructure. It also informs the critical infrastructure community and other stakeholders on how we intend to meet the objectives and mandates required by the Homeland Security Act of 2002, HSPD-7 (and any successor), the National Infrastructure Protection Plan, the Quadrennial Homeland Security Review, legislative requirements, and other authorities.

Our focus is to apply and promote innovative and leading-edge programs and activities that cost-effectively manage risk and enhance the resilience of the Nation's critical infrastructure. The relationships we build and the information we acquire about the efficacy of IP's programs in achieving desired outcomes will play an essential role in determining how we will invest future resources to address evolving needs and challenges. We must continuously adapt to changes in the risks to nationally significant critical infrastructure and address important dependencies, interdependencies, cascading effects, and supply chain impacts—including the impact of cyber incidents on critical infrastructure.

As we go forward, IP will build on its previous accomplishments and success. We will achieve our goals and objectives for critical infrastructure protection and resilience through a common set of outcomes against which we can prioritize and focus our efforts. We will support this with organizational excellence and the ability to innovate and adapt to future challenges.

2. Mission and Vision

The Homeland Security Act of 2002 defines the Department of Homeland Security's (DHS) responsibilities regarding the protection of the Nation's critical infrastructure. The national approach for critical infrastructure protection is provided through the unifying framework established in HSPD-7. This directive establishes the policy for enhancing protection of the Nation's critical infrastructure and, like the Homeland Security Act of 2002, mandates a national plan to implement that policy. The National Infrastructure Protection Plan (NIPP) currently fulfills this requirement.

HSPD-7 designates the Secretary of Homeland Security as the lead for critical infrastructure protection efforts. On the Secretary of Homeland Security's behalf, IP serves as the national coordinator for infrastructure protection, in accordance with the Homeland Security Act and HSPD-7. In addition, IP leads the Protection mission area under Presidential Policy Directive 8 (PPD-8) and coordinates with Federal agency leads across the other PPD-8 mission areas (Prevention, Mitigation, Response, and Recovery) to ensure a unified approach to national preparedness. IP also is responsible for leading and coordinating the implementation of counter-improvised explosive device policy.

IP has regulatory responsibilities as part of its critical infrastructure mission, specifically the Chemical Facility Anti-Terrorism Standards regulatory program, which establishes a risk-based approach to identifying and securing the Nation's high-risk chemical facilities. IP also manages the ammonium nitrate program.

IP's mission is complex due to the diversity, interdependent nature, interconnectedness, and ownership of the Nation's critical physical and cyber infrastructure. Most critical infrastructure located throughout our States and communities is privately owned and operated; therefore, public-private partnerships are essential to share information, understand interdependencies, protect infrastructure, respond to events, and build resilience.

The mission and vision for IP align with those for NPPD.

NPPD Mission	IP Mission
We lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.	Lead the national effort to protect critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community.
NPPD Vision	**IP Vision**
A safe, secure, and resilient infrastructure so that the American way of life can thrive.	Secure and resilient critical infrastructure across the Nation achieved through sound risk management, collaboration, information sharing, innovation, effective program management, and a highly skilled workforce.

A set of core values guides the way in which IP carries out its responsibilities and describes the operating environment we strive to create. These core values reinforce and expand upon NPPD's Leadership Covenant and its Guiding Principles.

NPPD Guiding Principles

ACCOUNTABILITY is demanded at every level of this organization. We pledge to ensure financial and managerial accountability in executing our, and our staff's, fiduciary responsibilities. As leaders, we are responsible for training, mentoring, and motivating our team, and we will be knowledgeable about and accountable for their work as well as our own. We will be ever mindful of the importance of our staff to the success of the NPPD mission.

PROFESSIONALISM is to be reflected in every action we take. We pledge to demonstrate the highest professional qualities and behavior in everything we do. We pledge to continuously improve our skills and those of our employees. We will actively engage and collaborate with our partners in training, planning, and operational activities to most effectively meet mission requirements.

RESPECT is fundamental to all levels of leadership, interpersonal relationships, and the working environment. We will treat our staff, peers, leaders, partners, and customers with a high level of respect and courtesy.

INTEGRITY is a vital element of our interactions and fundamental to all of our activities. We pledge to maintain the highest ethical standards and principles of public service and promote a culture of honesty and reliability.

COMMUNICATION is key to accomplishing our mission. As effective leaders, we will define our mission and openly and honestly communicate mission needs and goals. We will actively listen and provide feedback to our staff, team members, and peers.

EMPOWERMENT is essential for success. We will engage, value, motivate, and mentor employees to bring out their best. We will empower staff to utilize their unique skills, knowledge, and abilities to implement the NPPD vision and mission. When NPPD staff members do their best, we will acknowledge and affirm their contributions to the success of our Nation, the Department, and NPPD in a fair and equitable manner.

IP Core Values

Teamwork – Work collaboratively, openly, and honestly with our internal and external partners. Make decisions based on improved cross-division coordination and unity of effort.

Honor and Integrity – Be honorable in our work and maintain the highest ethical standards and principles of public service.

Professionalism and Respect – Demonstrate excellence and objectivity in everything we do. Respect the work and opinions of others, and encourage all personnel to provide constructive feedback while properly recognizing and rewarding superior achievements.

Accountability – Hold ourselves responsible for the outcomes of our actions, decisions, products, and behavior. When necessary, address performance issues in a timely, professional, and equitable manner that is in accordance with established DHS and Office of Personnel Management standards.

Stewardship – Effectively and efficiently utilize the resources entrusted to us to maximize the protection and resilience of the Nation's critical infrastructure and minimize duplication of effort through coordination with our DHS and Federal partners. Take actions to ensure that our protection and resilience efforts are focused on risk-informed priorities and measurable progress.

Empowerment and Growth – Take responsibility for personal and professional development and growth, accessing the training and resources needed to successfully fulfill our roles and responsibilities. Expand leadership and supervisory training and provide for the professional growth of all employees.

Communication and Information Sharing – Communicate openly and honestly with our partners and each other. Share information essential to carrying out our mission and achieving our goals, while safeguarding the critical infrastructure and personal information entrusted to us. Actively listen and provide feedback to our staff, team members, and partners.

Innovation and Adaptability – Explore and employ the most appropriate processes, programs, and technology to ensure sound risk management. Identify and examine alternatives to current approaches to ensure continuous improvement. Adapt and prioritize our efforts and resources in accordance with our strategy and the changing operating and risk environments.

3. IP's Approach to Risk Management: Goals and Objectives

The IP mission and vision are centered on managing risk. For IP, risk management consists of identifying and deterring threats, reducing vulnerabilities, and minimizing consequences. There are many types of risk—natural disasters, physical and cyber terrorist attacks, and manmade accidents. These risks have the potential of being exacerbated by changes in environmental conditions and failing infrastructure. In addition, risks are not realized uniformly; items of significant concern to a local community may not have impact beyond that community's boundaries while another risk of relatively minor local concern may have a major national or international impact. IP's primary (though not only) focus is on those risks to critical infrastructure with the potential for significant national impact—be they from intentional, accidental, or natural causes.

Risk may have impact far beyond the initial incident location due to the interwoven network of the Nation's critical infrastructure. This interconnectedness creates a vibrant private sector and provides the resilience to adjust to minor disruptions and incidents. However, the interconnected nature of critical infrastructure can also result in unanticipated and cascading impacts from events across infrastructure sectors and geographical areas. Increasing our understanding of these interconnections is essential to fully understanding and managing risk. So too, is continuing to work to promote the enhancement and modernization of infrastructure to limit the risk associated with aging, stressed, and failing infrastructure.

IP's mission and vision will be achieved by focusing our efforts on four goals that promote risk management. The goals listed below are described on the next four pages.

- Goal 1: Support and improve risk management activities across IP and the critical infrastructure community based on requirements and the best available information.

- Goal 2: Ensure effective coordination and information sharing with critical infrastructure partners to enhance protection and resilience activities during both normal operations and incidents.

- Goal 3: Increase awareness of and participation in IP's voluntary programs; implement regulatory programs to enhance critical infrastructure protection and resilience.

- Goal 4: Maintain a positive work environment that promotes achievement of organizational goals, collaboration, innovation, and professional growth.

Each goal is supported by a set of objectives (see pages 8-11) that describe how the goals will be accomplished between 2012 and 2016. Relevant members of Senior Leadership and parts of IP will be assigned to carry out these objectives to ensure completion and accountability. This section of the IP Strategic Plan outlines each goal, its objectives, and the underlying functions and capabilities needed to achieve the objectives.

IP's goals and objectives relate to the Quadrennial Homeland Security Review published in 2010, most significantly DHS Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events. Three of this goal's supporting objectives are particularly applicable to IP:

1) understand and prioritize risks to critical infrastructure;
2) protect critical infrastructure; and
3) make critical infrastructure resilient.

IP's activities also support additional DHS goals and objectives related to cybersecurity and resilience.

Goal 1: Support and improve risk management activities across IP and the critical infrastructure community based on requirements and the best available information.

Enabling the critical infrastructure community to manage risks to the Nation's critical infrastructure is central to IP's mission. Risk management is the process of identifying, analyzing, assessing, and communicating risk and managing it considering associated costs and benefits of any actions taken. While risk management principles acknowledge that risk often cannot be eliminated, effective risk management can mitigate risks and improve the quality of decisionmaking across the critical infrastructure enterprise. To this end, IP will employ a national risk management approach to guide policy, build effective programs, and support mission prioritization and resource allocation.

Using this risk management approach, IP will:

- Identify and understand critical assets, systems, networks, and their national and regional interdependencies;
- Use both internally collected and partner-shared information to assess, analyze, and prioritize risks to critical infrastructure across the Nation and within regions and sectors;
- Work with partners to align their respective goals and objectives to overall risk management priorities; and
- Measure progress and effectiveness and use results to prioritize risk management activities.

We will achieve this goal through the following objectives:

Objective 1.1: Conduct and guide national, regional, sector, cross-sector, and individual asset and system risk assessments.

Objective 1.2: Focus resources and efforts on prioritized risk management activities that measurably help to achieve defined outcomes.

Objective 1.3: Measure progress toward desired outcomes by demonstrating effectiveness of risk management activities.

Objective 1.4: Improve the analysis and understanding of physical system impacts from cyber and control system exploits to better manage them.

In collaboration with other parts of NPPD, particularly the Office of Cybersecurity & Communications and the Federal Protective Service, IP will enhance the integration of analysis, modeling, and assessment tools and methodologies to better analyze and understand the impacts on physical infrastructure from cyber and control system exploits and develop enhanced risk management solutions.

Continued collaboration with public and private sector stakeholders in the implementation of risk management strategies is central to attaining our goals. Such an approach will enable IP to remain responsive to the evolving needs of our partners so we can deploy appropriate tools and resources to support risk management strategies among the critical infrastructure community. In addition, in order to appropriately implement this framework, IP will apply a budget planning and resource allocation process that is responsive to risk priorities and the demonstrated effectiveness of our programs. The end result will provide IP with a holistic risk management framework that is repeatable, responsive to the changing risk environment, and focused on those areas where risk management strategies are most needed and most likely to be effective. The Assistant Secretary will make final resource allocation decisions based on a transparent and inclusive decision support process managed by the policy and management elements of IP.

Goal 2: Ensure effective coordination and information sharing with critical infrastructure partners to enhance protection and resilience activities during both normal operations and incidents.

The progress made to date in critical infrastructure protection and resilience owes largely to effective public-private partnerships. Working to involve the right people, continuing to forge and nurture trusted relationships across the partnership, and protecting the critical infrastructure and personal information necessary for collaboration remain top priorities for IP. To ensure the partnership continues to grow and provide maximum value, IP will strengthen coordination across critical infrastructure sectors and geographic regions. In a dynamic all-hazards environment, it is increasingly important to understand the growing interdependencies among the sectors and the cross-sector nature of industries and individual companies—along with how these linkages affect the management of national critical infrastructure risk. IP will continue to work closely with sector, regional, and cross-sector stakeholder groups in an effort to remain responsive to the needs of its partners across government and the private sector.

As the National Infrastructure Advisory Council has noted, "Information sharing is perhaps the most important factor in the protection and resilience of critical infrastructure." IP engages in and facilitates multi-directional information sharing with all its partners to ensure awareness of risks to critical infrastructure, during normal operations and incidents. IP provides its stakeholders, including the Nation's leaders, with timely and relevant information before, during, and after an incident to address which assets to protect, how to make operations more resilient, how to plan for potential disasters, when to ramp up to higher levels of security, and how to respond in the immediate aftermath of a disaster. IP will enhance the capability to maintain situational awareness and produce actionable information about physical and cyber risks to critical infrastructure by deepening the coordination and collaboration among the National Infrastructure Coordinating Center, the National Cybersecurity and Communications Integration Center, and the other DHS operations centers.

We will achieve this goal through the following objectives:

Objective 2.1: Strengthen, grow, and sustain broad public-private partnerships to enhance understanding of regional and cross-sector interdependencies and to capitalize on risk reduction opportunities.

Objective 2.2: Engage in multi-directional information sharing and provide stakeholders with timely and relevant information.

Objective 2.3: Strengthen coordination and collaboration with various DHS operations centers to promote unity of effort for incident management.

Objective 2.4: Expand the reach of IP programs, tools, and capabilities to provide information to help the critical infrastructure community manage risk and minimize the impacts of incidents.

Objective 2.5: Develop and implement a Strategic Communications Plan to inform and support coordination and information sharing with partners.

IP is expanding the national partnership framework by establishing public-private partnerships in regions around the country. A new Strategic Communications Plan will guide our communication-related activities and establish best practices. IP actively engages local partners through IP personnel located throughout the United States. These individuals are experts in assessing local and facility infrastructure risk and directly assist owners and operators and State and local officials in the utilization of IP programs and tools. IP prioritizes programs and capabilities that meet the stated needs of its critical infrastructure partners across the Nation. We work with partners in each Federal region as well as with Federal sector leads to assess regional risk, determine which IP programs are most useful to them, and identify gaps. Incorporating this information into its budget planning process enables IP to invest in those activities that help IP and its partners address gaps, grow and sustain the partnership, and effectively manage risk.

Goal 3: Increase awareness of and participation in IP's voluntary programs; implement regulatory programs to enhance critical infrastructure protection and resilience.

Both voluntary and regulatory approaches are essential to the success of critical infrastructure protection and resilience efforts. IP's regulatory programs provide vital information on some of the Nation's most significant chemical assets. Voluntary programs, on the other hand, are the foundation of IP's work with public and private sector partners to enhance the protection and resilience of the Nation's critical physical and cyber assets, systems, and networks.

Critical infrastructure owners and operators are generally in the best position to determine the cost-benefit tradeoffs of various security measures and take the appropriate actions. To assist in that effort, IP will continue to work with asset and system owners and operators, sectors, regional groups, and cross-sector groups to help them develop and promote their approaches for managing risk. IP must work to provide these partners with information on threats, consequences, vulnerabilities, interdependencies, technological solutions, and options for protective measures, based on effective practices, so partners can make decisions informed by costs and potential risk reduction benefits. IP will assess and promote resilience strategies; develop and share tools with critical infrastructure partners; conduct critical infrastructure-related education, training, and exercises; and offer expertise and best practices on risk mitigation approaches for critical infrastructure. IP will continue to develop and deploy capabilities to assist the critical infrastructure community to achieve desired national outcomes based on evolving requirements.

We will achieve this goal through the following objectives:

Objective 3.1: Enhance the protection and resilience of Level 1/Level 2 and other sector, State, local, tribal, and territorial infrastructure through IP programs that are coordinated and have measurable impact.

Objective 3.2: Share expertise and promote best practices in critical infrastructure protection and resilience.

Objective 3.3: Integrate voluntary sector-specific, asset-level, and other tools into a single assessment methodology.

Objective 3.4: Fulfill SSA responsibilities for Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, and Nuclear Sectors.

Objective 3.5: Implement Chemical Facility Anti-Terrorism Standards and Secure Handling of Ammonium Nitrate regulatory programs.

IP will integrate various voluntary sector-specific, asset-level, and other tools into a single assessment methodology to optimize the use of critical infrastructure data, particularly data visualization, and realize efficiencies for IP and our partners through improved internal and external coordination.

IP will continue to implement and enforce the regulatory programs for which it is responsible—the Chemical Facility Anti-Terrorism Standards and ammonium nitrate programs. IP will ensure regulatory requirements are met by sharing its expertise in implementing these regulations with the regulated community and also building broad-based awareness of its programs across the chemical industry. IP will also design and implement a consistent, defensible, and timely review process for Site Security Plans and Alternative Security Programs.

Across both the voluntary and regulatory environments, IP will coordinate efforts and initiatives internally to achieve desired national outcomes and greater efficiencies in working with the critical infrastructure community.

Goal 4: Maintain a positive work environment that promotes achievement of organizational goals, collaboration, innovation, and professional growth.

IP will maintain a culture that supports innovation and encourages collaborative efforts to achieve organizational goals while empowering the professional growth of its employees. A key element of this culture is frequent and open communication between Senior Leadership and employees—ensuring the participation of both headquarters and field-based personnel—to provide awareness on the status of IP initiatives and offer opportunities for employees to engage Senior Leadership and other colleagues from a variety of perspectives. Strong internal communication promotes innovative thinking and encourages contributions from across the organization, enabling IP to adapt and respond to the changing needs of its employees as its mission evolves.

IP will provide its workforce with the tools and resources necessary to achieve the goals and objectives set forth in this Strategic Plan. Each organizational element within IP has a mission and area of specialization that support the higher-level mission of IP. The overarching mission cannot be accomplished without the coordinated efforts of all the divisions working collaboratively toward the common goals and objectives of the organization. IP strives to eliminate barriers between its organizational elements so that no program or division operates in isolation but rather as part of a seamless whole. IP also coordinates closely with its partners across NPPD.

We will achieve this goal through the following objectives:

Objective 4.1: Facilitate regular, open, and honest communication across the entire IP workforce.

Objective 4.2: Ensure accountability for all IP activities to maintain the trust of the workforce and external stakeholders.

Objective 4.3: Develop and implement a Strategic Human Capital Plan to guide the recruitment of talented employees and ensure that IP provides training and career development paths for all employees.

Objective 4.4: Empower employees and promote unity of effort and cross-divisional coordination.

Objective 4.5: Foster coordination and collaboration across NPPD in operations, programs, and partner interactions.

By engaging broadly across the workforce, IP seeks to foster a sense of personal commitment to and professional investment in the organization and its mission. This supports a culture of responsibility and accountability for all IP activities on the part of Senior Leadership, other supervisors, and individual employees, building trust internally and with external stakeholders.

An effective organization prioritizes the professional development of its employees. In accordance with a new Strategic Human Capital Plan, IP will recruit talented employees and provide training and development paths for all employees, based on their job series and functional roles. This includes training and certification opportunities for managers and supervisors to enhance the quality and consistency of management experience across the organization. To the extent practicable, IP will offer training in a range of disciplines that spans the critical infrastructure mission space to support a broad knowledge base at all levels of the workforce. Temporary detail positions will allow employees to expand their experience, but will be balanced with the need to avoid disruptions to project teams. IP will use internal project management plans and performance appraisals to track and measure progress against the objectives.

4. Measuring Progress and Sharing Results

The Strategic Plan defines IP's vision for the future, our desired goals, and the objectives by which we will achieve those goals. On an annual basis, IP will release a brief update to this Strategic Plan to report on the progress that has been made against the goals and objectives. The update will draw on information from the Critical Infrastructure Protection and Resilience National Annual Report as well as additional reporting from IP's programs and activities. In particular, IP will use its set of internal project management plans—and the performance measures and metrics therein—to track and measure progress against the objectives. Starting in FY 2013, each project management plan will align to the relevant IP goals and objectives and develop performance measures and metrics that can be used to demonstrate progress on a monthly, quarterly, or annual basis—as applicable to each specific metric. The results will inform resource allocation and programmatic direction while providing guidance on what specific further actions are needed to ensure progress.

Measuring the impact of IP programs and policies in both a quantitative and qualitative manner is an essential element in the strategic planning process. The IP Strategic Plan promotes ongoing feedback on the progress IP and the critical infrastructure community are making with respect to risk management activities. This feedback is instrumental to IP making internal resource adjustments to address improvement opportunities.

The progress against IP's goals and objectives will also be integrated with other ongoing performance measurement and reporting efforts, particularly those put in place to support IP's national coordination role for critical infrastructure protection and resilience. In 2010, IP and its critical infrastructure partners—across government and in the private sector—began a collaborative effort (the Critical Infrastructure Risk Management Enhancement Initiative) to increase the value of annual reporting and performance measurement to enhance the effectiveness of the critical infrastructure community's collective risk management activities. Specifically, the initiative ensures that actions conducted to meet the requirements of the NIPP or its successor are developed and executed considering identified risks to critical infrastructure and their measurable impact on achieving particular outcomes.

A crucial first step was to collaboratively define a common set of outcomes for critical infrastructure protection and resilience. This resulted in a set of outcome statements that describe the desired "end state" for national critical infrastructure protection and resilience. Next, IP developed an integrated process to assess the current state of critical infrastructure protection and resilience against known risks, identify risk management efforts to address improvement opportunities, and then link those risk management efforts into programmatic and budgetary planning. We will use the outcome statements to measure progress and report objectively to Congress and other stakeholders on the national effort. This will support IP's internal effort to measure progress against this Strategic Plan.

Acronyms and Glossary

Acronyms

DHS	Department of Homeland Security
HSPD-7	Homeland Security Presidential Directive 7
IP	Office of Infrastructure Protection
NIPP	National Infrastructure Protection Plan
NPPD	National Protection and Programs Directorate
SSA	Sector-Specific Agency

Glossary

Critical Infrastructure: systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of those matters, across any Federal, State, regional, territorial, or local jurisdiction

Critical Infrastructure Community: Federal, State, regional, local, tribal, territorial, private sector, and other critical infrastructure partners and stakeholders

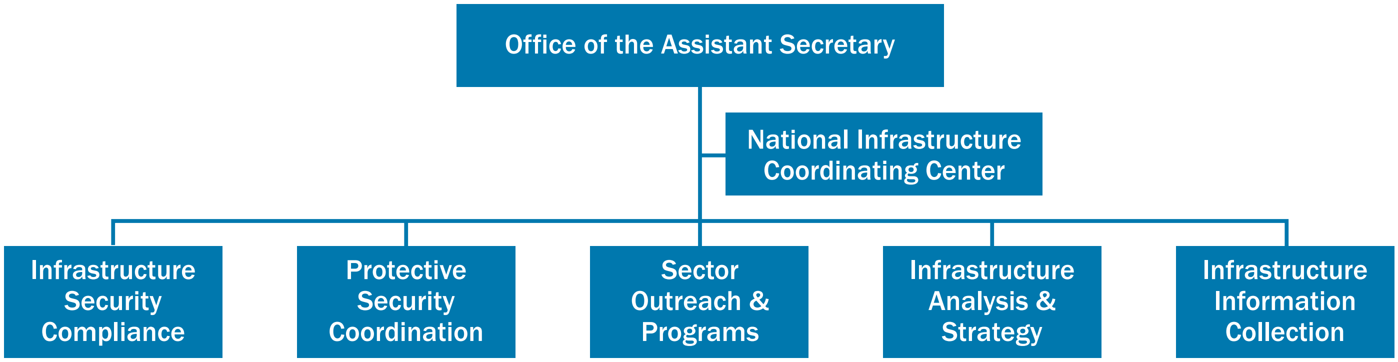
Level 1/Level 2: designations for those facilities whose destruction or disruption could have the greatest impact on a national, regional, or sector level

Resilience: ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions

Risk: potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences

Risk Management: process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken

Appendix A: IP Organization and Division Missions


Office of the Assistant Secretary
National Infrastructure Coordinating Center
Infrastructure Security Compliance
Protective Security Coordination
Sector Outreach & Programs
Infrastructure Analysis & Strategy
Infrastructure Information Collection

National Infrastructure Coordinating Center (NICC)

The NICC is the information and coordination hub of a national network dedicated to protecting the critical infrastructure of the United States by providing 24/7 integrated critical infrastructure support to DHS and critical infrastructure partners in order to reduce risk, prevent damage, and enable rapid recovery of critical infrastructure assets from incidents caused by all hazards.

Infrastructure Security Compliance Division (ISCD)

ISCD leads the efforts to secure America's high-risk chemical facilities and prevent the misappropriation of certain chemicals for use in terrorist acts on the homeland through the systematic regulation, inspection, and enforcement of Chemical Facility Anti-Terrorism Standards.

Protective Security Coordination Division (PSCD)

PSCD provides strategic coordination and field operations support to reduce risk to the Nation's critical infrastructure from a terrorist attack or natural disaster. PSCD executes five primary mission areas and one cross-cutting activity:

- Assessments (critical infrastructure and gap analysis)
- Outreach (steady-state and threat-based)
- Incident Response
- Special Events
- Training (risk mitigation and improvised explosive device (IED) awareness)
- Information Sharing & Coordination (cross-cutting activity)

Sector Outreach and Programs Division (SOPD)

SOPD executes the national effort to build, sustain, align, and leverage public-private partnerships with critical infrastructure stakeholders. Through strong collaboration with its partners, SOPD works across IP to develop and implement risk-informed programs that improve mitigation capabilities across the Nation, thus enhancing critical infrastructure protection and resilience.

Infrastructure Analysis and Strategy Division (IASD)

IASD provides strategic, operational, and tactical products and services to DHS and its partners through an analytic framework that integrates:

- Critical infrastructure and risk analysis across physical – cyber domains;
- Strategic, operational, and tactical risk analysis;
- Risk methodology development, modeling, and capabilities development; and
- Intelligence analysis and operations.

Infrastructure Information Collection Division (IICD)

IICD leads the Department's efforts to protect and provide standardized, relevant, and customer-focused infrastructure data to homeland security partners.

Homeland
Security