Department of Homeland Security
Office of Inspector General

# Protective Security Advisor Program Efforts to Build Effective Critical Infrastructure Partnerships: Oil and Natural Gas Subsector

OIG-11-12

November 2010

*Office of Inspector General*

**U.S. Department of Homeland Security**
Washington, DC 20528

Homeland
Security

November 12, 2010

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses the overall strengths and weaknesses of the DHS Office of Infrastructure Protection's Protective Security Advisor Program, and the program's role in protecting the Oil and Natural Gas Subsector infrastructure of the Energy Sector. It is based on interviews with employees and officials of relevant government agencies and private sector companies and organizations; direct observations; and a review of applicable documents and data. This report is one in a series of reviews of DHS' roles, responsibilities, and performance in the 18 critical infrastructure and key resources sectors.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Carlton I. Mann
Assistant Inspector General for Inspections

# Table of Contents/Abbreviations

Executive Summary ....................................................................................1

Background ....................................................................................2
CIKR Protection Strategies, Directives, and Legislation....................................................................................2
DHS' CIKR Integration Efforts....................................................................................4
Coordination, Collaboration, and Partnership ....................................................................................5
PSA Program Overview....................................................................................7
Oil and Natural Gas Subsector....................................................................................10

Results of Review ....................................................................................13
PSAs Develop Partnerships to Further Risk Reduction Efforts....................................................................................13
Stakeholders Consider PSAs an Effective Resource ....................................................................................15
Recommendation ....................................................................................26
Management Comments and OIG Analysis ....................................................................................26

A Well Defined and Communicated Mission Will Enhance Building Effective Critical Infrastructure Partnerships ....................................................................................28
Recommendations....................................................................................30
Management Comments and OIG Analysis ....................................................................................30

Coordination and Communication within DHS Needs Improvement ....................................................................................32
Recommendation ....................................................................................34
Management Comments and OIG Analysis ....................................................................................34

More PSA Program Support to Sector Leadership Partners is Needed....................................................................................35
Recommendations....................................................................................37
Management Comments and OIG Analysis ....................................................................................38

Current Metrics are Inadequate to Measure PSA Program Performance and Outcomes ....................................................................................40
Recommendation ....................................................................................43
Management Comments and OIG Analysis ....................................................................................44

Conclusion ....................................................................................45

## Figures

Figure 1: 18 Critical Sectors....................................................................................5
Figure 2: Map of PSA and IP Regional Director Distribution ....................................................................................8
Figure 3: PSA Partnerships to Risk Reduction....................................................................................14

## Appendices

Appendix A: Purpose, Scope, and Methodology ....................................................46
Appendix B: Management Comments to the Draft Report.......................................48
Appendix C: Sectors, Subsectors, and Sector-Specific Agencies..............................55
Appendix D: PSA Program Organization Chart .......................................................57
Appendix E: Energy Government Coordinating Council Membership.....................58
Appendix F: Oil and Natural Gas Sector Coordinating Council Membership..........59
Appendix G: Major Contributors to This Report ......................................................61
Appendix H: Report Distribution ..................................................................................62

## Abbreviations

| | |
|---|---|
| BZPP | Buffer Zone Protection Program |
| CIKR | Critical infrastructure and key resources |
| DHS | Department of Homeland Security |
| DOE | Department of Energy |
| ECIP | Enhanced Critical Infrastructure Protection Initiative |
| FEMA | Federal Emergency Management Agency |
| FOIA | Freedom of Information Act |
| GCC | Government Coordinating Council |
| IP | Office of Infrastructure Protection |
| NICC | National Infrastructure Coordinating Center |
| NIPP | National Infrastructure Protection Plan |
| NPPD | National Protection and Programs Directorate |
| OIG | Office of Inspector General |
| PCII | Protected Critical Infrastructure Information |
| PSA | Protective Security Advisor |
| PSCD | Protective Security Coordination Division |
| RRAP | Regional Resiliency Assessment Program |
| SAV | Site Assistance Visit |
| SCC | Sector Coordinating Council |
| SSA | Sector Specific Agency |
| TSA | Transportation Security Administration |

## Executive Summary

The Department of Homeland Security is responsible for protecting and strengthening resiliency of the nation’s critical infrastructure and key resources, which are assets, systems, and networks integral to the nation’s economy, security, and public health. As private industry owns and operates a significant portion of the nation’s critical infrastructure, the department emphasizes developing and sustaining public and private sector partnerships to secure and protect critical infrastructure. Within the department, the Protective Security Advisor Program develops these relationships and supports risk reduction activities.

We reviewed Protective Security Advisor Program activities to support the department’s mission to identify, prioritize, assess, and protect the nation’s critical infrastructure and key resources in the Oil and Natural Gas Subsector of the Energy Sector. We also reviewed program efforts to coordinate with subsector stakeholders to help strengthen critical infrastructure protection capabilities, identify vulnerabilities, and reduce risks.

Public and private stakeholders confirm that the Protective Security Advisor Program is an effective resource. As more innovative methods, techniques, and tools are developed, the program is adapting accordingly to meet the needs of department partners and to maintain program staff capabilities. While extensive stakeholder relationships and partnerships are developing at the state, local, and community levels, more attention is necessary to incorporate national level partners and stakeholders into strategic program planning. In addition, enhanced efforts to coordinate within the department and to collaborate with other federal partners would increase the program’s value to stakeholders.

We are making seven recommendations to improve the Protective Security Advisor Program’s effectiveness and to increase program coordination and communication with private and federal partners. In response to our report, the department has proposed plans and taken action that, once fully implemented, will reduce a number of deficiencies we identified. Department officials concurred with five of the recommendations and did not concur with two recommendations.

# Background

Critical infrastructure are assets, systems, and networks, both physical or virtual, which are so vital to the United States that incapacitation or destruction would debilitate security, national economic security, and public health or safety.  Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.  The federal government, state and local governments, communities, and private industry own and operate critical infrastructure and key resources (CIKR); however, the private sector owns a significant portion of CIKR.  Currently, there are 18 separate CIKR sectors, for which different federal agencies lead protection efforts.  These characteristics make CIKR protection a unique challenge that requires extensive coordination and partnership between and among the public and private sectors.

## CIKR Protection Strategies, Directives, and Legislation

The *Critical Infrastructure Protection Act of 2001*, acknowledged that the public and private sectors were interdependently linked through a network of critical physical and information infrastructures that only a continuous national effort could protect.[1]  In addition to establishing the current definition for critical infrastructure, this legislation mandated that all actions to limit or prevent exposure of these infrastructures to disruption occur through a public-private partnership.

In July 2002, the *National Strategy for Homeland Security* identified the nation's strategic homeland security objectives, and identified major initiatives within each to protect the nation's CIKR.[2]  It acknowledged that CIKR protection required compatible, mutually supporting strategies and efforts from government and the private sector.  Major initiatives outlined included developing a national plan to unify and coordinate the nation's infrastructure protection efforts; assessing all of the nation's CIKR to identify vulnerabilities; enabling the sharing, integrating, and protection of the sensitive information collected; and building collaborative partnerships between the federal, state, and local governments and the private sector.

[1] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, Public Law 107-56, Sec. 1016 (October 26, 2001).

[2] On October 5, 2007, the President's Homeland Security Council updated and reissued the *National Strategy for Homeland Security*.  It reflected new threat analyses, incorporated lessons learned from Hurricane Katrina and other catastrophic incidents, and described initiatives originating after the 2002 version as well as those under development for future deployment.

*The Homeland Security Act of 2002*, assigned the Department of Homeland Security (DHS) responsibility and authority to fulfill the CIKR missions defined in the *National Strategy for Homeland Security*.[3] The legislation also included the *Critical Infrastructure Information Act of 2002*.[4] This Act protects CIKR data voluntarily submitted to the government from disclosure under the *Freedom of Information Act*, state and local disclosure laws, and use in civil litigation or as the basis for regulatory action.[5] Pursuant to the *Critical Infrastructure Information Act*, DHS has developed and implemented the Protected Critical Infrastructure Information (PCII) Program, an information-protection program that enhances information sharing between the private sector and the government.

In February 2003, the release of the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* expanded on critical mission areas identified in the *National Strategy for Homeland Security*. It described an organizational structure designed to unify CIKR protection efforts, and established the framework for a public-private partnership. It also described specific roles and responsibilities for each partner, including DHS; lead departments and agencies; supporting federal agencies; state, tribal, and local governments, and private industry. In addition, the 2003 strategy identified key initiatives for each critical sector of the economy recognized in the *National Strategy for Homeland Security*, and for collaborative efforts in resolving issues crossing critical infrastructure sector and jurisdictional boundaries.

> "While it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the country, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur."
>
> *-- Homeland Security Presidential Directive-7, December 17, 2003*

In December 2003, *Homeland Security Presidential Directive*-7: Critical Infrastructure Identification, Prioritization, and Protection, established a national policy for collaborative efforts to protect the nation's CIKR. This directive assigned DHS the responsibility for coordinating the overall national effort to enhance CIKR protection and leading, integrating, and coordinating implementation efforts among federal departments and agencies; state, local, tribal, and territorial governments; and the private sector. In addition, the directive designated certain lead federal agencies as Sector-Specific Agencies (SSA), responsible for CIKR

[3] Public Law 107-296 (November 25, 2002).

[4] Title II, Part B of *The Homeland Security Act*, Public Law 107-296 (November 25, 2002).

[5] 5 U.S.C. § 552

protection activities in their designated sector. It also mandated that DHS and the SSAs coordinate with the private sector to identify, prioritize, and coordinate CIKR protection, and to facilitate information sharing about threats, vulnerabilities, incidents, potential protective measures, and best practices. The directive required DHS to produce an integrated national plan for CIKR, and to implement all systems and procedures for sharing and protecting CIKR-related information among federal, state, and local governmental entities, and the private sector.

## DHS' CIKR Integration Efforts

Founded on the public-private partnership concept, and building upon these previous CIKR policies and strategies, DHS issued the *National Infrastructure Protection Plan* (NIPP) in June 2006, and updated it in February 2009. The NIPP specifies a framework for increasing security and resiliency of the nation's CIKR through understanding and sharing information about terrorist threats and other hazards; building security partnerships to share information and implement CIKR protection programs; implementing a long-term risk management program; and maximizing efficient use of resources for CIKR protection. The NIPP defines processes, methods, tools, and relationships that security partners and stakeholders need to achieve these objectives. DHS' Office of Infrastructure Protection (IP) uses the NIPP framework to lead the coordinated national effort to reduce the nation's CIKR risk, and to work toward a safe, secure, and resilient national infrastructure based on and sustained through strong public and private partnerships.

The NIPP describes 18 "logical collections of assets, systems, or networks that provide a common function to the economy, government, or society," or critical sectors.[6] See Figure 1 for a list of the sectors, and Appendix C for a more detailed description of each sector. The sectors encompass all aspects of the American economy and way of life: essential goods and services, governmental institutions, national defense industries and contractors, connecting data and communications, and economic and business structure services. Many of the sectors cover large, diverse industries, that, although they all provide common services to society, have different needs, approaches, vulnerabilities, and security solutions. In some cases, sectors are broken down into subsectors to address these differences.

[6] *National Infrastructure Protection Plan*, February 2009.

## Sector-Specific Agency Roles

DHS is the SSA for 11 of the 18 CIKR sectors (See Figure 1), and coordinates the protection of the seven remaining sectors.

SSAs work with DHS, through IP, to implement the NIPP; form partnerships with relevant federal, state, local, and private sector entities; cultivate information sharing and analysis; develop protective programs and strategies; and provide guidance as needed. SSAs also provide, arrange, or facilitate sector-specific training, domestic incident management and preparedness activities, and interdependency and consequence analyses. Each SSA is responsible for developing, implementing, and maintaining a sector specific plan that describes the sector's ongoing and future protection initiatives. In addition, SSAs assess sector progress and report the results to DHS in sector-level annual reports and in periodic performance feedback reports.

**Figure 1: 18 Critical Sectors**

**CIKR Sectors**

Banking and Finance
**Chemical ***
**Commercial Facilities ***
**Communications ***
**Critical Manufacturing ***
**Dams ***
Defense Industrial Base
**Emergency Services ***
Energy
Food and Agriculture
**Government Facilities ***
Healthcare and Public Health
**Information Technology ***
National Monuments and Icons
**Nuclear ***
**Postal & Shipping ***
**Transportation Systems ***
Water

*** DHS has SSA Responsibility**

*Source: NIPP, February 2009*

# Coordination, Collaboration, and Partnership

While DHS leads the national CIKR protection efforts, coordinating and collaborating with relevant stakeholders is essential. These stakeholders and partners include the companies and trade associations within the private sector; public entities responsible for emergency or incident management and homeland security; and federal entities that regulate or partner with the private sector and state CIKR programs. The NIPP presents an organizational structure known as the sector partnership model that provides stakeholders with a defined process for coordinating, exchanging information, joint planning, and providing information on and analysis of governmental efforts and initiatives. The model includes overlapping coordinating and advisory councils led by public and private sector partnerships, with guidance, tools, and support from DHS.

IP collaborates with the 18 sectors mainly through the Sector Coordinating Councils (SCC), which are the principal sector policy coordination and planning entities. Each SCC is self-organized, self-run, self-governed, and independent of the federal government. It is composed of sector stakeholders reflecting the sector's composition, including owner/operator representatives of facilities, major corporate entities, and trade associations representing companies of varying sizes. In some cases, SCCs exist for subsectors. For example, within the Energy Sector, the Oil and Natural Gas Subsector has an SCC. The SCCs provide forums for private industry to identify and implement effective information-sharing capabilities; organize and coordinate sector policies in planning and preparedness, exercises and training, public awareness, and NIPP implementation activities; integrate public sector plans with private-sector initiatives; and provide input to the government on sector research and development efforts and requirements.

Building partnerships represents the foundation of the national CIKR protection effort. These partnerships provide a framework to:

- Exchange ideas, approaches, and best practices;
- Facilitate security planning and resource allocation;
- Establish effective coordinating structures among partners;
- Enhance coordination with the international community; and
- Build public awareness.

*-- NIPP, February 2009*

Stakeholders also interact through a variety of other councils. For example, the Government Coordinating Council (GCC) is the public sector counterpart to the SCC and is co-chaired by SSA and IP leadership.[7] The Critical Infrastructure Partnership Advisory Council affords all of the SCCs and GCCs a forum to engage in joint discussions and activities that have national, all-sector effect; and through the CIKR Cross-Sector Council SCC leaders explore cross-sector and interdependency matters. The Government Cross-Sector Council, which includes the NIPP Federal Senior Leadership Council and the State, Local, Tribal, and Territorial Government Coordinating Council, facilitates communication, collaboration, and coordination among the GCCs and other federal and non-federal public sector entities.[8] In addition, the Regional Consortium Coordinating Council provides a forum for those with regionally based interests in CIKR protection, involving multi-jurisdictional, cross-sector, and public-private sector efforts focused on the preparedness, protection, response, and recovery of infrastructure and the associated economies within a defined population or geographic area.[9]

[7] IP's Sector-Specific Agency Executive Management Office carries out SSA responsibilities for six of the 18 CIKR sectors: Chemical; Commercial Facilities; Critical Manufacturing; Dams; Emergency Services; and Nuclear Reactors, Materials, and Waste.

[8] The NIPP Federal Senior Leadership Council consists of leadership representatives from the SSAs as well as other federal agencies with interests relevant to CIKR protection and resiliency. The State, Local, Tribal, and Territorial Government Coordinating Council consists of homeland security directors or their equivalents from state, local, tribal, and territorial governments.

[9] Members of the Regional Consortium Coordinating Council include regional partnerships, groupings, and governance bodies. Because coordination across government jurisdictions is crucial, the Chair of the State, Local, Tribal, and Territorial Government Coordinating Council is also a standing member.

## PSA Program Overview

IP's mission is to lead the national effort to mitigate terrorism risk to, strengthen the protection of, and enhance the all-hazard resilience of the Nation's critical infrastructure. Within IP, the Protective Security Coordination Division (PSCD) is responsible for assessing vulnerabilities and consequences; developing, implementing, and providing national coordination for protective programs; and facilitating CIKR response and recovery operations in an all-hazards environment to reduce risk to the nation's CIKR. The Division's Field Operations Branch manages the Protective Security Advisor (PSA) Program to assist PSCD in carrying out these responsibilities.

The PSA Program supports DHS' CIKR efforts by encouraging state, local, tribal, and territorial governments, and private CIKR owner/operators to participate and collaborate within the NIPP risk management framework. The PSAs are DHS' on-site critical infrastructure and security specialists assigned at the local level throughout the United States. Through the coordination of vulnerability assessments, incident support, and information sharing, PSAs seek to improve the security posture of the stakeholders.

The program began as a pilot in 2004, with one PSA who met with state Homeland Security Advisors and other stakeholders to determine needs and expectations for DHS field-level CIKR protection specialists. Based on the response from those meetings, the program added PSAs in early 2005 and developed further. From FY 2005 to FY 2010, the program increased from 56 to 93 PSAs. PSAs are deployed to 70 districts, and the program has a budget of more than $12 million for FY 2010.[10] As of September 2010, the program had at least one PSA in all 50 states and Puerto Rico, eight IP Regional Directors, and six PSA positions at headquarters.[11]

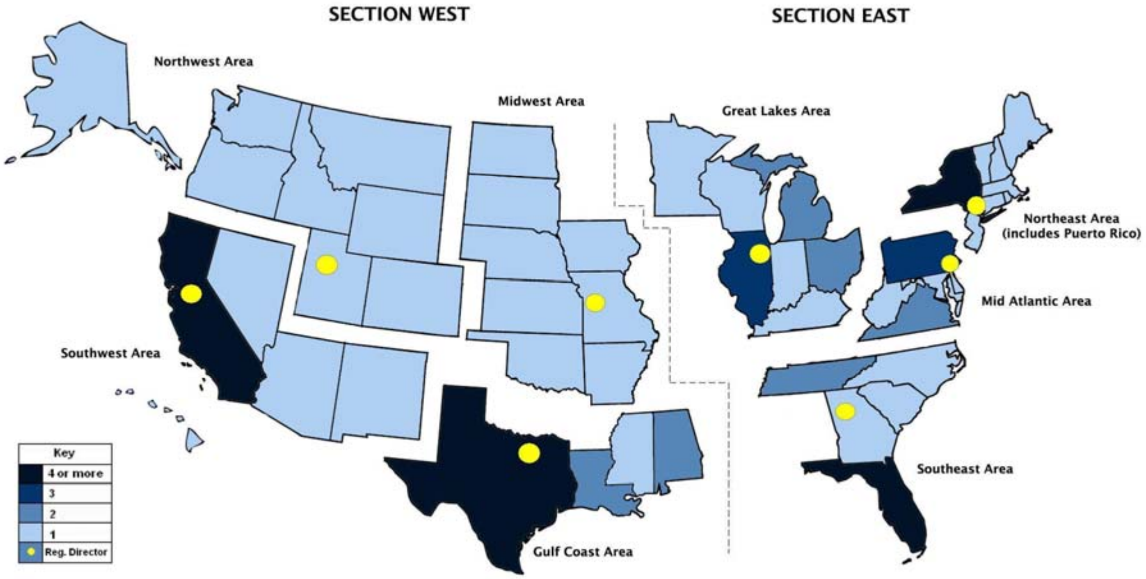
The PSA Program has two geographic sections, the East and West, each managed by one Section Chief. Both sections have four designated regions, and one IP Regional Director manages each region. IP Regional Directors report to their respective Section Chief and manage PSA activities in their region. Figure 2 depicts the PSA and IP Regional

[10] Districts include a combination of entire states, portions of states, and major metropolitan areas. Several PSAs share duties in a number of large cities, as needed to provide adequate coverage for the distribution of CIKR, while other PSAs cover the remaining portions of the state.

[11] IP Regional Directors function as Supervisory PSAs and are included in the cadre of 93 PSAs.

Director national distribution as of September 2010. An organization chart showing PSA staff distribution is in Appendix D.

**Figure 2: Map of PSA and IP Regional Director Distribution**



*Source: OIG analysis of information provided by IP, September 2010.*

Stakeholders expect PSAs to know intimately the districts they serve. As such, program-hiring officials look for prospective candidates with specific background, experience, and relationships already established in particular geographic areas. Current PSAs average more than 20 years experience in military, counter-terrorism, or law enforcement, are specialists in security with critical infrastructure experience and knowledge, and are not necessarily specialists in any particular sector. As PSAs work with stakeholders in all 18 sectors, the position requires a thorough understanding of programs that affect critical infrastructure within DHS and in other agencies, or a significant foundation upon which to build such knowledge.

PSA training requirements are structured and delineated in a multi-year Learning Roadmap. The Roadmap defines five levels of advancement and achievement for PSAs, each with specific required training and optional areas of study. It includes required basic knowledge and skills, such as relevant policies, tools, and programs, and progressively builds on that knowledge base to develop specializations and areas of expertise. The training includes courses and instruction developed internally by IP, as well as from a variety of federal agencies and private organizations, including DHS' Federal Emergency Management Agency (FEMA), DHS' Federal Law Enforcement Training Center, and ASIS International.

The program also maintains membership for all PSAs in ASIS International, an international organization for security professionals, and encourages PSAs to pursue professional certifications ASIS International offers, such as the Certified Protection Professional and Physical Security Professional.

PSAs function as the department's field liaisons and coordinators to support critical infrastructure protection efforts. These efforts involve collaborating with private industry, state and local governments, and federal partners. PSAs are building and maintaining information-sharing partnerships; coordinating or performing site vulnerability assessments and surveys; and assisting during incidents. After establishing a relationship with a stakeholder, the PSA functions as a liaison between that organization and IP, and often facilitates access to other DHS components, or to state and regional agencies. Although the PSAs build relationships with stakeholders in all sectors, a PSA may work primarily in the sectors whose infrastructure is the dominant concern for the state, geographic area, or district they serve.

## Tools and Resources

The PSA Program has a variety of technological, human, and physical resources that enable PSAs to respond to and interact with geographically dispersed stakeholders across the nation and program officials in headquarters. For example, the PSAs use a web-based, central data warehouse developed to track their activities as well as maintain a knowledge base on the nation's critical infrastructure. This system maintains the PSAs' schedules and activities, which allows program officials to respond timely to questions from stakeholders and DHS leadership about ongoing fieldwork or work on certain CIKR efforts. PSAs can quickly upload incident status updates, report on affected facilities, and assist in prioritizing efforts based on the facility's capabilities and its local, regional, and national criticality.

Program leadership attributes much of the PSA Program success to the centralized support provided by its Duty Desk. The Duty Desk, located at headquarters, provides 24-hour support to the PSAs and answers both administrative and technical questions. The Duty Desk also tracks and assigns tasks and information requests from DHS leadership and other stakeholders. In addition, the Duty Desk coordinates requests to provide speakers at various events or locates appropriate DHS officials outside of IP.

The Field Operations Branch's Field Support Section within PSCD coordinates headquarters support for the PSAs. This includes administrative and project management assistance, property management support coordination, IT support coordination, logistics, and data analysis and reporting. Because of the PSAs' extensive travel, the branch dedicates two Field Support Team staff to organize travel and maintain travel records to support PSAs.

## Oil and Natural Gas Subsector

The Energy Sector consists of thousands of geographically dispersed electricity, oil (petroleum), and natural gas assets. A myriad of systems and networks in most of the nation's states and territories connect them. A wide variety of public and private entities own, operate, and regulate these assets. Because the activities and assets supporting electricity resources infrastructure differ significantly from those for oil and natural gas in extraction/generation, production, transport, distribution, and storage, each is separated into subsectors within the Energy Sector. The Department of Energy (DOE) is the SSA for the Energy Sector and its Oil and Natural Gas and Electricity Subsectors.

The oil and natural gas industry is an example of a CIKR subsector that engages PSAs throughout the nation and requires coordination among many entities. The Oil and Natural Gas Subsector is functionally diverse, consisting of pipelines, control systems, above- and below-ground storage facilities, refineries, processing plants, and marine ports, as well as offshore and onshore fields and facilities. To secure and monitor its production cycle, the industry relies on a series of complex systems that involve physical and virtual capabilities for processing, refining, storing, and distributing or transporting fuel products. As an older and heavily regulated industry, the Oil and Natural Gas Subsector has mature mandatory and voluntary security policies and processes, which it implements independently, through industry associations, and with governmental oversight.

**U.S. Oil and Natural Gas Statistics [January 2010]**

| | |
|---|---|
| Number of Operable Refineries | 150 |
| Oil, Natural Gas Pipeline Mileage | 2,534,000 |
| Oil, Natural Gas Imports [barrels/day] | 10,487,000 |

*Sources: Energy Information Administration;*
*Pipeline and Hazardous Materials Safety Administration, Department of Transportation*

## Oil and Natural Gas Subsector Stakeholders

Within the Oil and Natural Gas Subsector, public-private partnerships address security issues of concern to the subsector, and share information on threats, vulnerabilities, and protective measures.  The Oil and Natural Gas SCC represents private sector security partners.  The SCC membership includes 23 trade associations and represents approximately 98% of the industry's owner/operators.  A list of Oil and Natural Gas SCC members is in Appendix F.

The Oil and Natural Gas Subsector relies heavily on Transportation Systems Sector infrastructure, including pipelines, freight rail, and maritime facilities.  Because of these interdependencies, the Oil and Natural Gas SCC established the Pipeline Working Group, which also acts as a Pipeline SCC within the Transportation Systems SCC.  This group allows the two SCCs to coordinate on oil and natural gas transportation security issues, and reduces duplicative meetings and efforts.

In addition, many energy-related facilities and infrastructure also operate as chemical or hazardous materials facilities, creating interdependencies with the Chemical Sector.  The Oil and Natural Gas SCC and Chemical SCC have formed joint working groups to discuss and make recommendations on issues of mutual concern, to include emergency management and metrics.

There are also numerous national and regional associations and working groups with state and local official participation.  These organizations coordinate activities and emergency response, and develop policies that affect oil and natural gas security.  Further, private industry stakeholders have formed Facility Security Officer working groups, the Energy Security Council, and Internal Security working groups.  Through these groups, members are able to network and share best security practices to enhance the overall security posture of the industry.  In addition, some groups often invite federal and state partners, such as the Federal Bureau of Investigation and state Homeland Security Agencies, to participate.

Regulatory organizations with roles in the various aspects of the oil and natural gas industry cover municipalities, cities, states, regions and federal offices, commissions, agencies, and departments.  The industry's many diverse facilities and commodities are separately regulated and have multiple stakeholders and trade associations.  In addition, governmental agencies at the state, local, tribal, and federal levels are responsible for emergency planning, incident management, homeland security, and for preventing and responding to energy supply, demand, and pricing concerns.

The Department of Transportation's Pipeline and Hazardous Materials Safety Administration and the Pipeline Security Division of DHS' Transportation Security Administration's (TSA) Office of Transportation Sector Network Management are responsible for the operational safety and security of the oil and natural gas pipelines used to transport raw and refined fuel products. The Pipeline and Hazardous Materials Safety Administration develops uniform standards and administers the national regulatory program to assure the safety of pipeline transport of natural gas, petroleum, and other liquid hazardous materials. TSA's Pipeline Security Division endeavors to enhance the security preparedness of the nation's pipeline systems through security programs; assessments, reviews, and analysis; and sharing industry best practices and lessons learned. The two agencies executed a formal agreement in August 2006 to delineate lines of authority and responsibility; and to establish guidelines for cooperation, collaboration, and information sharing to ensure coordinated, consistent, and effective activities, as well as no duplication of effort.

The U.S. Coast Guard regulates the ports, vessels, and waterfront facilities used by the Oil and Natural Gas Subsector to ship or receive bulk shipments. These ports, vessels, and facilities must meet the requirements for security assessments and security plans implemented because of the *Maritime Transportation Security Act of 2002*.[12] This Act established a consistent national security program by requiring port, facility, and vessel assessments and plans that include such measures as screening and personnel identification procedures, security patrols, access control, and collaboration through area committees. The U.S. Coast Guard promulgates and enforces regulations, policies, and directives implementing the Act's provisions; reviews security and incident response plans; conducts assessments; and ensures alignment with existing domestic maritime regulations and directives.

We reviewed how PSA Program operations and activities support DHS' mission to identify, prioritize, assess, and protect the nation's CIKR in the Oil and Natural Gas Subsector of the Energy Sector. We also reviewed the program's role in coordinating with subsector stakeholders to help strengthen critical infrastructure protection capabilities, identify vulnerabilities, and reduce risks.

[12] Public Law 107-295 (November 25, 2002).

# Results of Review

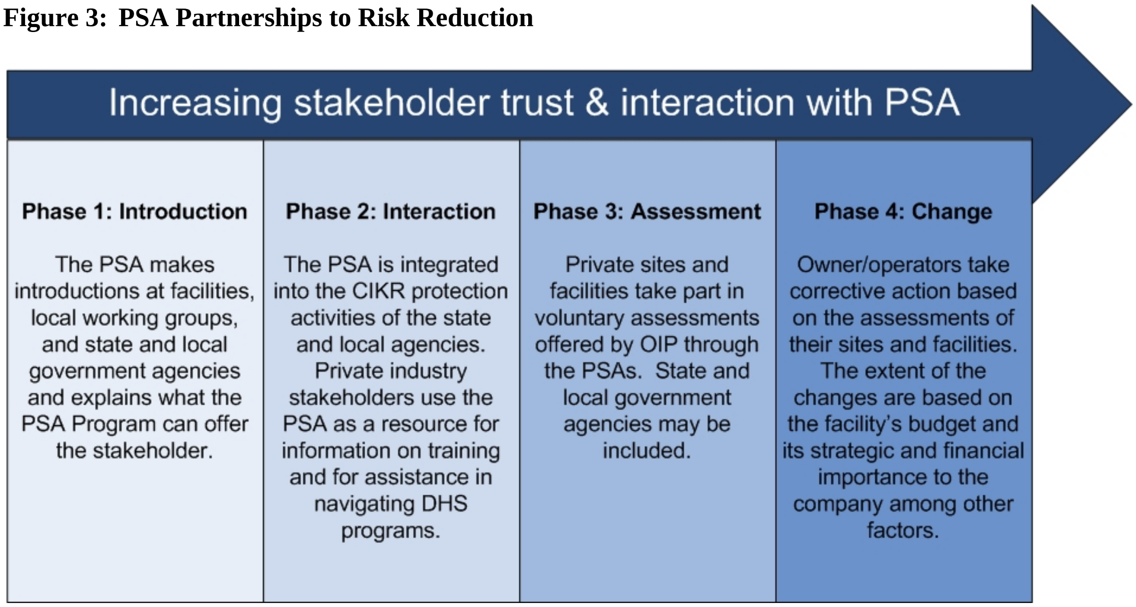
PSAs develop relationships with private sector stakeholders to encourage mitigation and risk reduction actions at critical sites and facilities. PSAs also build partnerships with public sector stakeholders in state and local CIKR programs to assist and facilitate implementing the NIPP, including identifying, prioritizing, assessing, and securing public and private sector critical sites and facilities. Although PSA activities align with DHS' mission and the partnership model stated in the NIPP, there is no clearly defined mission statement directing PSA Program activities, and PSAs are unable to articulate effectively the program's full value to public and private stakeholders. Unclear goals and objectives are also causing tension within DHS and with other governmental partners, as PSA activities and relationships appear to overlap, duplicate, or conflict with critical protection efforts of other entities. Lastly, the program needs to develop metrics properly suited to measuring outcomes achieved, while taking into account the diversity of each sector and jurisdiction.

## PSAs Develop Partnerships to Further Risk Reduction Efforts

PSAs develop relationships with private sector stakeholders to encourage mitigation and risk reduction actions at critical sites and facilities. We separate the evolution of these relationships into four distinct phases—introduction, interaction, assessment, and change—and public and private stakeholders identified different benefits and some challenges at each phase. The PSA Program can improve the value realized in each phase by defining and communicating a clearer results-oriented mission and by improving its coordination and communication efforts with sector partners.

From our interviews with a wide variety of stakeholders, PSAs develop stakeholder relationships in progression to further risk reduction efforts, and the evolution involves initial contact and introduction; increased engagement and interaction; assessments; and ultimately effecting change through stakeholders voluntarily implementing enhanced security measures. Figure 3 describes this progression. Differences in states, facilities, and sectors influence how quickly a PSA can progress relationships from the introduction phase, to the interaction and assessment phases, and eventually effect change.

**Figure 3: PSA Partnerships to Risk Reduction**



Increasing stakeholder trust & interaction with PSA

**Phase 1: Introduction**

The PSA makes introductions at facilities, local working groups, and state and local government agencies and explains what the PSA Program can offer the stakeholder.

**Phase 2: Interaction**

The PSA is integrated into the CIKR protection activities of the state and local agencies. Private industry stakeholders use the PSA as a resource for information on training and for assistance in navigating DHS programs.

**Phase 3: Assessment**

Private sites and facilities take part in voluntary assessments offered by OIP through the PSAs. State and local government agencies may be included.

**Phase 4: Change**

Owner/operators take corrective action based on the assessments of their sites and facilities. The extent of the changes are based on the facility's budget and its strategic and financial importance to the company among other factors.

*Source: OIG Analysis*

During the introduction phase, the PSA makes contact with stakeholders, either independently or through other established contacts. The PSA is building a network of contacts across sectors, companies, and public agencies by working directly with state and local government officials; conducting outreach calls and visits to agencies and facilities; attending meetings of regional, state, local, community, and industry organizations; and delivering briefings to introduce and advertise the PSA Program and DHS CIKR efforts. Stakeholders become aware that the PSA is available as a security resource, and DHS establishes initial stakeholder connections, creating an environment for future partnership.

In the interaction phase, stakeholders, both public and private, use the PSA as a resource. The PSA and stakeholders communicate frequently on training opportunities and threat information as allowable. Stakeholders introduce the PSA to other contacts and invite participation in meetings and exercises. Stakeholders communicate PSA capabilities and resources available, further developing the PSA's network. PSAs assist stakeholders in making valuable contacts with other federal, public, and private CIKR partners. The PSA is also an integral part of incident and event management. DHS receives additional benefits because the PSA can contact stakeholders for immediate situational awareness during incidents. DHS also gains state and local insight on the criticality of certain assets to specific regions and the Nation.

The assessment phase involves the PSA conducting or coordinating vulnerability assessments. These assessments include preparations for Special Security Events and incident response.[13] Both public and private stakeholders gain third party insight on the security posture of sites, facilities, and communities; empowering stakeholders to implement changes. DHS gains additional insight on national risk and interdependencies, and progresses toward its ultimate goal of risk reduction.

The change phase is the point where the stakeholder voluntarily implements enhancements to its security posture. CIKR owner/operators at the corporate and facility levels address vulnerabilities identified through PSA assessments, thereby reducing risks and mitigating threats.

## Stakeholders Consider PSAs an Effective Resource

We interviewed public and private stakeholders in the oil and natural gas industry, as well as various state and local CIKR protection partners. Regardless of the phase, stakeholders described relationships with designated PSAs and services provided as valuable.

**Phase 1: Introduction**

The PSA makes introductions at facilities, local working groups, and state and local government agencies and explains what the PSA Program can offer the stakeholder.

**<u>Phase One: Introduction</u>**

Many PSAs described stakeholder introductions as crucial to developing a foundation for relationship progression, and rely on these relationships. These relationships allow PSAs to provide services, collect data on CIKR protective efforts, expand networks, and get information quickly to DHS senior leadership during an incident or event. Although a number of PSAs had established contacts and ties to communities before joining the program, PSAs build new relationships. In many cases, a PSA’s credentials, experience, approach, and work ethic help establish common ground with facility security managers. To gain trust, acceptance, and to be of value, stakeholders said PSAs need a humble demeanor, an eagerness to learn the industry, and should be open and responsive. Stakeholders considered a PSA most effective when willing to assist, while not being demanding or disrespectful of the stakeholder’s time.

[13] Special Security Event is a DHS designation for an event that requires federal resources and unique security plans and training because of anticipated dignitary attendance, event size, and event significance.

Most stakeholders said a PSA with law enforcement and military background is critical in establishing common ground with security managers, as facility security managers often have similar experience. Stakeholders said PSAs do not need to be sector experts, but need security expertise, an awareness of all pertinent facilities, an understanding of the area's geography, and a basic understanding of a facility's significance to the region and Nation.

Smaller Companies and Less Mature Sectors May Develop Relationships More Rapidly

The majority of oil and natural gas industry owner/operators have mature security procedures, with security personnel and operators who have been securing facilities around the world for years. As a result, the industry does not typically ask for assistance, which makes transitioning to further relationship phases more challenging. Some industry representatives suggested that because so many larger oil and natural gas companies have the financial resources and have been building their security measures for years, smaller companies as well as sectors less accustomed to infrastructure protection have a greater need for PSA services. In some cases, one person might manage the infrastructure protection at a facility, and starting and maintaining a more extensive infrastructure protection program could be cost and resource prohibitive. The free services the PSA advertises during the introduction phase might be more attractive to certain facilities, and those relationships may progress more rapidly.

## Phase Two: Interaction

**Phase 2: Interaction**

The PSA is integrated into the CIKR protection activities of the state and local agencies. Private industry stakeholders use the PSA as a resource for information on training and for assistance in navigating DHS programs.

The interaction phase was most often described by stakeholders as important, since it provides access to no-cost services that help improve stakeholder security posture and capabilities without initial capital investment. Immediate access to CIKR or related information, intelligence, threats, training, and industry standards, is available through the PSA. PSAs also connect stakeholders to services from other DHS components, thereby serving as a *one-stop shop*. DHS gains increased engagement with critical infrastructure owner/operators, according to the NIPP concepts of partnership and collaboration. This improves the communication and information sharing necessary for national infrastructure protection.

In addition, a number of stakeholders said there are not enough PSAs nationwide, citing reduced personal attention. Although most stakeholders lauded their PSAs' responsiveness, some said PSAs are not always available and increased demands on the PSAs without an increase in the PSA cadre could negatively affect PSA interaction phase activities. Although developing a relationship with a PSA was essential to trusting the PSA Program as a whole, stakeholders said their relationship was with the program and not necessarily with a particular PSA. Should a current PSA leave, stakeholders recommend a period of overlap between the current PSA and the new PSA to help ensure a smooth transition. In response to the report, PSA Program officials responded that this practice is not possible under current federal hiring processes and Office of Personnel Management regulations.

To address transition issues, however, the PSA Program has established procedures to mitigate potential gaps in coverage experienced by a departing PSA. For example, when a PSA leaves, the program directs another PSA or multiple PSAs from neighboring districts to assume responsibility for the affected district. The program introduces new PSAs to stakeholders prior to a PSA's departure to familiarize stakeholders with the new PSA, formalize responsibility transition, and ensure continuity of effort.

### PSAs Assist Stakeholders to Ensure Staffs Are Adequately Trained

Stakeholders often ask PSAs about training opportunities for the private sector and state and local officials. In addition to online courses on topics such as community hurricane preparedness, available through FEMA, IP offers training courses targeted to security managers, and can send teams to facilities to perform these trainings at the stakeholders' request. Examples of the security training offered include surveillance detection courses and private sector counterterrorism awareness workshops. As the federal government funds those resources, the educational opportunities promoted and coordinated through PSAs are advantageous to stakeholders.

Some industry stakeholders receive regular updates on educational opportunities from their PSAs, and have participated in recommended courses, conferences, and seminars. As funded or inexpensive targeted training for industry professionals has become more difficult to find, having PSAs notify stakeholders of any private industry-focused security training opportunities is useful. Some stakeholders, however, expressed frustration that private security managers do not have access to potentially beneficial training courses only available to governmental professionals.

PSAs Play a Significant Role in Incident and Event Management

For incidents and national profile security events, PSAs provide support to local, state, and federal emergency management teams. They also provide timely status information to DHS' National Infrastructure Coordinating Center (NICC) and IP leadership concerning CIKR facilities.[14] In addition, PSAs coordinate with multiple entities to help private industry get facilities back online quickly after an incident. PSAs are often the first DHS employees on the scene in response to an incident. In combination with the relationships built before an incident, PSAs can provide rapid situational awareness to DHS and IP officials, and serve as an information coordinator and needs liaison with local, state, federal, and private sector stakeholders after an incident.

PSAs have access to state and local official distribution lists to allow for immediate response, have a collaborative relationship with FEMA on incident response issues, and provide assistance when requested. When an incident occurs or is imminent, the state's Emergency Operations Center generally manages the incident response, and PSAs report to the center and deploy as necessary. From these locations, PSAs leverage their relationships with private industry stakeholders to provide information to the state's Emergency Operations Center, the NICC, and IP leadership on the status of specific critical facilities. PSAs are also able to advise state and local stakeholders on specific facility vulnerabilities, and help determine priorities for protection or deploying resources.

For example, a number of stakeholders praised the PSAs' incident management activities, especially during recovery efforts for Hurricanes Ike and Gustav in 2008. Stakeholders said PSAs served as a direct line to funnel CIKR information and updates to DHS and the NICC, and as a single point of contact for private industry's CIKR related needs. PSAs helped private sector facilities restore operations and leveraged relationships with local

[14] The NICC is a 24-hour watch/operations center that maintains operational, situational, and incident awareness of the nation's CIKR sectors. The center provides for centralized coordination and exchange of threat, alert, warning, incident, event, and other relevant information among the public and private sectors.

law enforcement officials, the state, and other agencies to facilitate private industry employee re-entry to disaster-affected areas.

### Stakeholders Value PSA Information Sharing Activities

PSAs facilitate information sharing daily; program officials estimate that information sharing is 50% to 60% of a PSA's job. Across the Nation, PSAs participate in at least 52 different Oil and Natural Gas Subsector security working groups and councils. To ensure PSAs maintain relationships with as many stakeholder groups as possible, some work with state homeland security and emergency management officials to attend meetings, taking each other's messages to the meetings, and then briefing one another on the proceedings.

Upon request, PSAs also provide private industry and some state and local officials with threat information. As each relationship is different, a PSA might automatically provide one stakeholder with any relevant threat information, while waiting for a request from another. When permissible, PSAs inform facilities how to determine whether they are under surveillance, how to identify the signs of other dangerous activities, and how the facility can employ protection measures. In addition, PSAs share any daily publicly available information, in some cases extracting and sharing only the protective information of interest to a security manager based on current events, the site, or location.

Stakeholders use the PSAs to obtain information on a variety of topics, including proposed legislation and best practices. In some instances, other entities contact a facility for information, and the facility owner/operators call PSAs to vet the requesters. Some stakeholders use the PSAs to get information on an event occurring in another area where they may have facilities. A common complaint, however, was that the information sharing was sometimes one-sided, and sometimes not expedient. In addition, some stakeholders note a considerable decline in information sharing since the program's inception, however, it was unclear whether this was a result of modified policies within IP or reduced information available to PSAs.

### Stakeholder Information Sharing Has Improved, but Concerns Remain

The background, approach, and interactions PSAs have with industry stakeholders are significant in determining whether stakeholders are willing to work with the program. However, another indispensible factor to information sharing is building trust in the PCII Program. A PCII designation protects business-sensitive, security related facility, company, and industry documents, records, or other data voluntarily submitted to DHS from disclosure. Initially, most sectors and subsectors classified CIKR reports, which hindered information sharing and best practices exchanges among the stakeholders. Because of a PCII designation, PSAs can disseminate general, sanitized reports about sector and subsector issues as For Official Use Only, while protecting any specific facility information and data provided by the private sector from disclosure.

Private industry stakeholders and associations suggested that, in combination with the relationships built with their PSAs, the PCII Program helps facilitate the flow of information in an industry known for a reluctance to share information. In addition, the PSAs regularly attend many of the same meetings and working groups of stakeholders, and share contacts with the private industry, and vice versa. Industry stakeholders said that this constant interaction and exposure has increased trust and fostered relationships. Because of this, facilities grant PSAs access more quickly to help identify vulnerabilities.

For other stakeholders, however, concerns remain about divulging too much information. A common concern voiced was an uncertainty about what DHS was doing with data it collected during facility assessments, and whether DHS could use this information against the stakeholders in the future. Despite protections guaranteed by the PCII Program, stakeholders still have data use and storage concerns.

### PSAs Support State and Local Government CIKR Programs, But Better Understanding of Government Programs is Necessary

PSAs bring additional CIKR-dedicated human and technological resources to state and local governments, especially during incident response. In many states, officials describe PSAs as a part of their team and include PSAs in state agency meetings. Some state partners use PSAs to help bridge relationship gaps between them and private industry. Because of the current economic environment and diminished state and local resources, some states use PSAs more to assess and strengthen CIKR protection activities. However, most state officials we spoke with were concerned that

PSAs cannot currently provide enough support to compile CIKR lists for state use and for submission to DHS.

In most states, the partnership between the PSA and the state's CIKR program focuses on the owner/operators, with the state and PSAs presenting a consistent message to facilities. Working as a team alleviates additional burdens on facilities; companies are more receptive to this approach, often allowing the team to share security-related information.

State officials said they want PSAs to have a better understanding of all state and federal programs that relate to the Oil and Natural Gas Subsector, not just those within IP or DHS. It would be more useful for PSAs to know what the industry already does with other assessments, inspections, studies, or evaluations before requesting potentially duplicative information and data.

Some state officials also expressed the need for better communication between DHS headquarters and PSAs, specifically regarding the submission of CIKR for DHS' critical asset lists. While the PSAs offer states assistance in compiling the lists, the PSAs are often unable to explain the criteria or identify an IP representative who can explain why some assets are included on the Level 1/Level 2 list and why some are not.[15] Concerning additional support needed from PSAs, some states want to use the PSAs more for state CIKR data call submissions to DHS and for asset prioritization. In response to the report, PSA Program officials disputed this assertion and indicated it is a misunderstanding of the PSAs' role in the CIKR data call.

The PSAs' role is to assist states in compiling the lists by helping state personnel identify infrastructure critical to that state, and to verify facility data, e.g., physical address, geospatial coordinates, name. PSAs are not involved in establishing criteria, or the determinations to include or not include facilities on the final prioritized list of critical infrastructure, as this is the function of IP's Infrastructure Analysis and Strategy Division.

[15] Level 1/Level 2 (formerly called Tier 1/Tier 2) ranking is part of DHS' National CIKR Prioritization Program, identifying nationally significant critical assets and systems. This annual identification relies heavily on the insights and knowledge of a wide array of public and private sector security partners. DHS uses the rankings to determine eligibility and implementation of certain CIKR protection programs and initiatives, such as grant programs, buffer zone protection efforts, facility assessments, training, and other activities. The Level 1/Level 2 list is classified.

Some state officials thought it might be worthwhile to have a PSA that focused on certain sectors and for more PSAs to be involved in smaller events or incidents that do not reach the level for federal assistance.  Other state officials suggested a PSA working strictly on state legislature issues and located in the state's capitol would be worthwhile.

## **Phase Three:  Assessment**

**Phase 3: Assessment**

Private sites and facilities take part in voluntary assessments offered by OIP through the PSAs.  State and local government agencies may be included.

Vulnerability and risk assessments performed for stakeholders by DHS components identify security weakness areas and possible options for critical infrastructure security improvements.  This guidance is extremely valuable as private sector stakeholders and state and local jurisdictions aim to minimize and limit expenditures.  Developing stakeholder cooperation and collaboration is crucial to DHS building the national database of risk areas and inventory of critical infrastructure.  It also provides DHS with information necessary to plan for the use of resources such as grant programs, research and development, exercises, and additional training course development.  Any specific facility information and data provided by the private sector and collected by IP during these assessments holds a PCII designation, which typically exempts it from disclosure.

Private Sector Owner/Operators Consider Voluntary Assessments Valuable

The PSAs conduct and coordinate vulnerability surveys and assessments for private sector facilities.  These assessment services could cost as much as $25,000 when obtained privately, but are made available to the stakeholders at no cost.

*Site Assistance Visits*

Site Assistance Visits (SAV) are voluntary.  PSAs coordinate with PSCD's Vulnerability Assessment Branch to conduct an SAV.  The assessment team is composed of three to four individuals with specialized skills and knowledge specifically suited to the facility type and location.  Most teams include bomb, technical, and assault planning experts.  During these assessments, the team simulates likely threat scenarios to determine where security vulnerabilities exist and to develop mitigation strategies.  Some facility security managers said the teams were sometimes so knowledgeable about a facility's technical operations it was necessary to contact engineers and other staff to respond to team questions.

The Vulnerability Assessments Branch conducts 250-300 SAVs per year.  An SAV requires 1-3 days to complete, depending on its focus.  The assessment team provides the owner/operator with an initial assessment, and follows up with written report within 90 days.  Stakeholders have full discretion to act or not act on report recommendations.

*Enhanced Critical Infrastructure Protection Initiative*

While the SAV provides a more comprehensive look at facilities' vulnerabilities and can be tailored to focus on specific aspects of critical operations such as cyber and control systems, the Enhanced Critical Infrastructure Protection (ECIP) Initiative is a voluntary data collection and outreach program.  The ECIP provides the PSA with an opportunity to educate facility owner/operators on security, and to promote communication and information sharing among facility owner/operators, DHS, and state and local government agencies.  The PSA works with the facility's security manager to document the physical security, security force, security management, information sharing, protective measures, and dependencies that exist at a facility.  PSAs collect data using a standardized survey and this data is compiled into a Protective Measures Index.  The index is a quantitative protection measure developed for each of the 18 different sectors, which allows for security measures comparison with other similar facilities in the same sector and subsector.

After the survey, the owner/operator receives the results in the form of an ECIP Dashboard, which is an interactive electronic reporting tool that provides a current picture of the facility's Protective Measures Index information, as well as a graphic comparison of the facility's index to other similar facilities.  The ECIP Dashboard allows the stakeholder to manipulate its security posture variables and to determine how to improve protection in a cost effective manner by prioritizing capital expenditures.  Stakeholders value the ability to make comprehensive comparisons of their facility to similar facilities.  These tools also allow DHS to map facility, sector, and subsector interdependencies, and determine whether resiliency exists.  Therefore, the survey not only serves as a strong relationship-building tool, but also allows for data gathering on infrastructure protection levels in general.

### States Benefit From Assessment Programs

While vulnerability assessments often take place on privately owned infrastructure, states and local jurisdictions also benefit from assessment programs that provide funding and help communities prepare for incidents at facilities in their jurisdictions.

#### *Regional Resiliency Assessment Program*

The Regional Resiliency Assessment Program (RRAP) is a voluntary IP-led interagency assessment of selected CIKR, along with regional analysis of the surrounding infrastructure. The RRAP identifies CIKR dependencies, interdependencies, cascading effects, resiliency characteristics, gaps, and the prevention and protection capabilities of owner/operators, local law enforcement, and emergency response organizations.

Coordinated by PSCD and the PSAs, the RRAP is a collaborative effort of IP that includes other federal agencies, public homeland security officials, state and local government, and private-sector owner/operators, working to enhance resilience of the CIKR and surrounding communities. Some states may not be able to perform similar assessments as efficiently and effectively without funding.

After the RRAP review, IP analyzes the information, determines gaps in response capabilities, coordination and resources, and documents the results in a written report. This information is provided to the state's homeland security agency and participating facilities. For example, a recent RRAP in New Jersey involved 18 sites in a ten-mile radius, and included at least 27 ECIPs and 18 SAVs. With this regional approach, the RRAP review can provide a more complete assessment of resiliency, interdependency, and security. RRAP projects take 3 to 6 months to execute, are very collaborative, and attempt to leverage each organization’s capabilities. Five RRAP projects were conducted in FY 2009, and during our fieldwork, PSCD was finalizing the 2010 projects.

#### *Buffer Zone Protection Program*

Administered by FEMA, the Buffer Zone Protection Program (BZPP) complements IP’s Vulnerability Assessments Branch SAVs. While assessment visits recommend protections and preparedness measures inside a facility’s perimeter, the BZPP addresses protections and preparedness levels for the surrounding area and emergency responders outside the facility.

The BZPP provides grant funding to increase the protection, preparedness, and response capabilities of communities that contain certain Level 1/Level 2 CIKR. The BZPP provides $50 million in grants annually to cover approximately 200 assets. BZPP funding is allocated to states or territories based on the number, type, and character of pre-identified higher-risk sites within their respective jurisdictions. Funds are then further distributed to community law enforcement and first responders who react to incidents at those facilities. PSAs often help jurisdictions apply for and conduct BZPP assessments. In addition, some PSAs conduct ECIP surveys simultaneously with BZPP assessments, providing the facility with the benefit of the ECIP Dashboard, and the jurisdiction with the ability to apply for funding to respond to emergencies at the facility.

### Regulatory Obligations May Hinder the PSA Relationship Building Progress

A perception that oil and natural gas industry regulation already exists may hinder stakeholder program participation. Some industry stakeholders said they do not take advantage of SAVs because of previous experiences with the department, and because stakeholders have existing obligations and reporting requirements to DHS and other governmental regulatory programs. Other stakeholders declined to participate in voluntary site visits and assessments because they are already overwhelmed with DHS regulations concerning chemical facility standards, transportation worker identification, and other programs.

However, other stakeholders said the PSA Program bridges a gap between DHS' regulatory side and maintaining relationships to help owner/operators protect facilities. For example, several stakeholders have notified and invited their PSA, as an independent observer, when another federal or state agency is conducting an inspection, assessment, or exercise. Although these stakeholders have not progressed to the assessment phase, they said PSA Program services could be valuable, and would engage the program more should corporate headquarters change policy.

**Phase 4: Change**

Owner/operators take corrective action based on the assessments of their sites and facilities. The extent of the changes are based on the facility's budget and its strategic and financial importance to the company among other factors.

**Phase Four: Change**

Through efforts in the previous three phases, PSAs work towards having owner/operators implement risk reduction activities and improve protective measures at facilities. However, many factors outside of the PSA's control influence whether a private sector facility will make any voluntary security enhancements. Some stakeholders stated that even though they knew the assessment recommendations were valid and useful, voluntary changes ultimately depend on financial resources and the strategic importance of a facility to the company.

While many stakeholders take advantage of PSA coordinated services and assessments and have made significant steps toward implementing recommendations, the PSA Program does not have structured follow-up that tracks activities to determine what influence the program has had on risk reduction. To evaluate the change effected by the PSA Program, the program needs to track and record stakeholders efforts, develop methods to compile sufficient information for DHS to evaluate the national CIKR risk posture, and use that information to inform PSA Program resource efforts and future planning.

## Recommendation

We recommend that the Director of the Protective Security Coordination Division:

**Recommendation #1:** Develop a process to track and record voluntary assessment recommendation implementation, and use this information to guide future PSA Program recommendations, resource efforts, and planning.

## Management Comments and OIG Analysis

We evaluated NPPD's written comments and have made changes to the report where we deemed appropriate. A summary of NPPD's written response to the report recommendations and our analysis of the response follows each recommendation. A copy of NPPD's response, in its entirety, is included as Appendix B.

We also received technical comments from the PSA Program and the Department of Energy and incorporated those technical changes into the report where appropriate. We appreciate the comments and contributions made by each entity. NPPD/IP concurred with five of our recommendations and did not concur with two recommendations.

**Management Response:** NPPD/IP concurred with Recommendation 1. NPPD officials responded that the PSA Program already has established processes and metrics to track voluntary implementation of security and resilience improvements resulting from IP assessments. The PSA Program has implemented 180-day follow-up interviews to capture information on risk-reduction implementation activities following PSA conducted ECIP security surveys. As facilities receive subsequent ECIP surveys, additional data collected will inform the change effected by the PSA Program. The 180-day follow-up currently identifies improvements made or implemented to physical security, security force, security management, information sharing, protective measures, and dependencies.

NPPD officials responded further that in June 2010, using the ECIP security survey and 180-day follow-up data, PSCD analyzed voluntary protective measure implementation at facilities receiving ECIP visits. This metric was the first ever produced demonstrating the effect of the PSAs and ECIP security surveys. Based on initial analysis of implementation data, IP is developing new performance metrics that will reflect implementation of improvements to security and resilience resulting from voluntary IP assessments.

NPPD will incorporate the 180-day follow-up process into other IP assessments, namely the SAV. Through the 180-day follow-up process and subsequent assessments of those same facilities, IP will be able to capture and track improvements over time, providing a better understanding of how the PSA Program, IP, and NPPD are buying down risk for the Nation’s critical infrastructure. The facility security and resilience data, and voluntary implementation data captured by these IP assessments will allow DHS to evaluate the national protection posture of critical infrastructure, and inform NPPD, IP, and PSA Program goals, future planning efforts, and resource allocations.

**OIG Analysis:** We consider NPPD/IP's proposed actions responsive to Recommendation 1, which is resolved and closed. No further reporting on this recommendation is required.

## A Well Defined and Communicated Mission Will Enhance Building Effective Critical Infrastructure Partnerships

Although PSA activities align with DHS' mission and the partnership model described in the NIPP, there is no clearly defined mission statement directing PSA Program activities. To measure the effectiveness of PSA activities, the program needs to identify and develop achievable milestones, based on results-oriented goals and objectives. Unclear goals and objectives are also causing tension with other governmental partners, as PSA activities and relationships appear to overlap, duplicate, or conflict with critical protection efforts of other entities. The majority of Oil and Natural Gas Subsector stakeholders said they are uncertain of the PSA Program's overall mission. However, most stakeholders understand the role PSAs have in building and maintaining relationships and partnerships with the private sector; working with industry on assessing its exposure to threats and vulnerabilities; and addressing questions and providing information on DHS programs and operations.

### <u>PSA Activities are Aligned with Organizational Mission and Goals</u>

DHS is working to reduce the Nation's vulnerability to terrorist attacks, major disasters, and other emergencies. To do so in part, DHS' FY 2008-2013 Strategic Plan identifies the goal of protecting CIKR and an accompanying objective of protecting and strengthening resilience through the department's efforts. These efforts include mitigating potential vulnerabilities and fostering partnerships to safeguard against the most dangerous threats and risks to CIKR.

The department's goal of protecting critical infrastructure is delegated from NPPD to IP; protecting CIKR through risk reduction is then delegated to PSCD. Within PSCD, the PSA

Program intends to assist fulfilling this goal by aligning its activities with NPPD and IP objectives.  These activities include:

- Establishing partnerships with stakeholders; consolidating preparedness assets from across DHS and facilitating grants;
- Supporting first responder training, citizen awareness, public health, infrastructure, and cyber security; protecting high-risk targets;
- Providing timely, actionable, and valuable threat information;
- Implementing and maintaining a fully operational incident management capability;
- Enhancing public and private sector self-sufficient risk reduction activities; and
- Developing and implementing effective protective programs to reduce risk to CIKR assets, systems, networks, and functions.

To determine whether these PSA activities are contributing to DHS' mission, the program needs to identify its own mission, and develop achievable milestones, based on results-oriented goals and objectives.

### Unclear PSA Program Mission Limits Ability to Develop Stakeholder Relationships and Partnerships

With only an implied mission related to individual PSA activities, the PSA Program is currently unable to identify what it intends to accomplish.  Several government and private stakeholders expressed that the program's mission was never clearly defined or communicated.  As a result, intended goals are unclear and there is difficulty determining roles and responsibilities, which creates overlap and some frustration.  A clearly defined mission is necessary for building relationships and partnerships with stakeholders.

For example, ineffective initial communication and coordination among program offices strained the relationship between DOE and the PSA Program.  DOE officials said there have been some overall coordination improvements with the PSA Program. Previously, very little to no advance notice was given to DOE when PSAs went to Energy Sector assets and owner/operators, but this is improving.  DOE officials also said the roles and responsibilities between IP and the SSAs need better definition, particularly in sectors where DHS is not the SSA, such as the Energy Sector.

In addition, a clear and communicated PSA Program mission could help stakeholders manage expectations, as well as understand the activities and expertise of the PSA cadre. For example, some stakeholders and federal partners do not recognize or understand the distinction in roles between the PSA Program and the Vulnerability Assessments Branch concerning survey and assessment resources. While the PSA coordinates SAVs, the Vulnerability Assessments Branch conducts these assessments. Not understanding the PSAs' role causes some stakeholders to question whether PSAs have the sector specific expertise necessary to conduct SAVs, even though PSAs do not conduct SAVs.

While the activities and responsibilities of the PSAs align with IP, NPPD, and DHS missions, evaluating the PSA Program as effective or ineffective without a stated mission and related objectives is difficult. A clearly stated program mission, with objectives and intended outcomes, will clarify PSA roles and responsibilities for CIKR partners and stakeholders.

## Recommendations

We recommend that the Director of the Protective Security Coordination Division:

**Recommendation #2:** Develop a mission statement for the PSA Program, and communicate the mission within DHS, to public and private stakeholders, SSAs, and other federal CIKR partners.

**Recommendation #3:** Develop achievable PSA Program milestones, based on results-oriented goals. Goals and objectives should align with and influence achieving IP, NPPD, and DHS CIKR goals and objectives.

## Management Comments and OIG Analysis

**Management Response:** NPPD/IP concurred with Recommendation 2. NPPD officials responded that PSAs do have a clearly defined mission statement, described in the PSA Program Management Plan. The PSA's mission statement is to "R*epresent DHS and IP in local communities throughout the United States*."

The PSA mission is to work with State Homeland Security Advisors' offices and their security partners throughout the region, serving as liaisons between DHS; the private sector; and federal, state, territorial, local, and tribal entities and acting as the DHS onsite critical infrastructure and vulnerability assessment specialists.

NPPD officials responded further that PSAs are able to articulate the program's mission to stakeholders, and that stakeholders understand the program's affect and value individually. However, stakeholders do not perceive the broader, national level impact of coordinated PSA activities across the country. NPPD officials said the issue is not the lack of a mission statement, but rather mission messaging to stakeholders such that stakeholders understand the national level purpose and mission of PSA activities, and how those activities link with activities of other federal agencies and programs with similar responsibilities. The PSA Program will communicate to stakeholders the PSA Program's intended results and overall mission better.

**OIG Analysis:** We consider NPPD/IP's proposed actions responsive to the intent of Recommendations 2, which is resolved and open. The recommendation will remain open pending our receipt of the PSA Program's strategy and implementation plan to communicate intended program results and its overall mission to stakeholders better. The communication strategy and implementation plan should include communication activities within DHS, to public and private stakeholders, SSAs, and other federal CIKR partners.

**Management Response:** NPPD/IP responded that it non-concurs with Recommendation 3. Officials said the PSA Program has reached a degree of operational maturity where it is no longer focused on milestones, which are typically related to program establishment, e.g., creating an IP/PSA presence in every state. The PSA Program has matured and has developed performance metrics to measure the results of its efforts, which align with and influence achieving IP, NPPD, and DHS goals and objectives. Program officials said further detail on these metrics is included in its response to Recommendation 7.

**OIG Analysis:** Although NPPD/IP did not concur with this recommendation, we consider the proposed actions responsive to Recommendation 3, which is resolved and open. This recommendation will remain open pending our receipt of approved multi-year performance metrics and associated results-oriented performance goals that demonstrate achievement of the PSA Program's mission; and that such efforts align with IP, NPPD and DHS CIKR goals and objectives as referenced in IP's responses to Recommendation 1 and 7.

## Coordination and Communication within DHS Needs Improvement

Within DHS, multiple components regulate and collaborate with the public and private sectors to protect CIKR. The number of assessments and requests for similar information from the department creates frustration within private industry, especially in the oil and natural gas industry where many governmental entities have safety, security, or oversight responsibilities. DHS' internal coordination issues diminish the PSA Program's value and improved collaboration is necessary to serve CIKR stakeholders and partners more efficiently and effectively.

### Stakeholders Express Need for Better Coordination

Multiple stakeholders said the oil and natural gas industry's primary issue with the PSA Program is the need for coordination between the different partners, and the program's value diminishes when DHS offices and components do not communicate effectively. In November 2009, DHS' Secretary met with the Oil and Natural Gas SCC leadership, among others, to discuss critical infrastructure security. The SCC leadership reiterated its need for DHS to resolve internal coordination issues. While the industry realizes agencies have different missions and mandates, better coordination would reduce confusion among oil and natural gas owner/operators.

As mentioned previously, some stakeholders have PSAs attend regulatory inspections or routine safety reviews as an objective observer. There are planned events, inspections, and reviews where coordination between DHS components could improve. For example, FEMA conducted a tabletop exercise in which numerous DHS components helped plan and subsequently participated. However, PSAs were neither informed nor invited to attend. As a result, shortly after the exercise started, stakeholders and other participants questioned why PSAs were not present. Even though the oversight was resolved quickly, it highlights the need for more effective communication within the department.

## Assessments are Performed by Several DHS Components

The Oil and Natural Gas Subsector is heavily regulated, therefore increased coordination and transparency is necessary. Stakeholders said information often requested by one program is similar to information already provided to another program. Stakeholders want programs to exchange information rather than answer the same questions multiple times. Many stakeholders have a long working history with federal agencies, and they are less concerned with sharing information among agencies than the costs of redundant assessments and information requests.

Stakeholders referred to the multiple regulatory assessments currently performed by DHS, including those under Chemical Facility Anti-Terrorism Standards as well as the U.S. Coast Guard's Maritime Security directives and regulations pertaining to the *Maritime Transportation Security Act of 2002*. The Chemical Facility Anti-Terrorism Standards are mandatory for any facility that manufactures, uses, stores, or distributes certain chemicals at or above a specified quantity. IP's Infrastructure Security Compliance Division is responsible for carrying out the regulatory assessments, promoting collaborative security planning, and ensuring that covered facilities meet the risk-based performance standards. The U.S. Coast Guard issues Maritime Security Directives mandating specific security measures for vessels and facilities when additional security measures are necessary to respond to a threat assessment or to protect from a specific threat against maritime elements of the national transportation system.

Further, TSA's Pipeline Security Division conducts Corporate Security Reviews to evaluate incident plans, programs, and implementation. The Pipeline Corporate Security Review Program is an on-site review of a pipeline operator's security plan and its implementation, conducted by TSA's Pipeline Security Division staff. The review uses a standard protocol to capture quantitative and qualitative data that aid in prioritizing critical systems and in establishing a baseline against which to evaluate minimum-security standards in the industry and identify coverage gaps. In addition, TSA conducts legislatively mandated Critical Facilities Inspections; however, participation by facilities in these reviews is voluntary, as are any actions recommended as a result of inspections.[16] Stakeholders question why components within the same department do not share this security information.

Although there is some duplication in assessments performed on facilities concerning security, some stakeholders said that each assessment has a different focus in addition to security. A number of stakeholders said PSA assessments are attractive because they are free, non-consequential, and provide third party credibility to requests for security upgrades. Some stakeholders view assessments negatively as they are very time consuming and work-intensive for their staff. Therefore, it would be helpful to stakeholders to have common security related assessment information coordinated ahead of time.

## Recommendation

We recommend that the Director of the Protective Security Coordination Division:

**Recommendation #4:** Inventory regulatory and voluntary assessments, reviews, and resources of tribal, local, state, and federal governmental entities that affect Oil and Natural Gas Subsector stakeholders, and determine where the PSA Program can leverage efficiencies and enhance coordination.

## Management Comments and OIG Analysis

**Management Response:** NPPD/IP concurred with Recommendation 4. IP management responded that it agrees a comprehensive inventory of these items would be beneficial to PSAs to improve their sector knowledge. However, development of such an inventory is not the responsibility of the PSA Program or PSCD. Responsibility for maintaining this level of awareness of relevant assessments, reviews, and resources affecting sectors lies with the SSAs. Sector Specialists from IP's Partnership and Outreach Division will work with DOE to create a consolidated

[16] The *Implementing Recommendations of the 9/11 Commission Act of 2007,* Sec. 1557, Public Law 110-53 (August 3, 2007), requires TSA to develop and implement a plan for reviewing pipeline security plans and inspecting the critical facilities of the 100 most critical pipeline operators as identified by a September 2002 Department of Transportation circular.

inventory of the regulatory and voluntary assessments, reviews, and resources that affect Oil and Natural Gas Subsector stakeholders. The PSA Program will support IP's Partnership and Outreach Division in this endeavor to create the inventory, and once completed, will determine where the PSA Program can leverage efficiencies and enhance coordination. When the PSA Program knows of assessments, reviews, and resources, officials responded that the program already coordinates with relevant stakeholders and works to create efficiencies.

**OIG Analysis:** We consider NPPD/IP's proposed actions responsive to Recommendation 4, which is resolved and closed. No further reporting on this recommendation is required.

## More PSA Program Support to Sector Leadership Partners is Needed

DHS has a responsibility to support and coordinate effectively with all SSAs. PSA interactions with stakeholders across the nation provide DHS with a unique opportunity to support ongoing SSA efforts to implement the NIPP in each sector, especially for SSAs with limited resources to maintain a similar continuous field presence. By effectively communicating with the SSA during strategic planning, the PSA Program can better align its assistance to support DOE. In addition, the PSA Program can benefit from increased interaction because of the vast sector-specific technical knowledge DOE possesses. Further, increased coordination with the Oil and Natural Gas SCC and greater presence at meetings would strengthen stakeholder and PSA Program communication, allow PSAs to be involved in strategies outlined in sector specific plans, and increase PSA Program awareness of issues and needs.

### PSA Program Can Improve DHS' Support of DOE

As the SSA, DOE is responsible for implementing the NIPP framework and guidance as tailored to the specific characteristics and risks of the Energy Sector as a whole, and the Oil and Natural Gas Subsector specifically. DHS' role is to help coordinate with and support DOE in its efforts to lead, integrate, and coordinate the activities of the sector and subsector, as well as providing guidance, tools, and analytical support to the SSA and its sector/subsector membership.

PSAs have a geographic advantage over some SSAs, as PSAs are field-based and interact with stakeholders directly, whereas some

SSAs are headquarters-based and would need to send staff to conduct field assessments and visits. DOE officials said they want to be involved in the assessment programs, but do not have additional dedicated resources to participate in most PSA field assessments and visits.

Because DOE is unable to participate in most cases, officials are concerned about PSA interactions with stakeholders and information collected. For example, when PSAs first began performing ECIPs, the program did not communicate with DOE on ECIP objectives, what assessments it was conducting, and on which facilities. DOE officials said they would prefer more coordination and interaction with the PSA Program to facilitate mutual objectives, as DOE is unsure of PSA expertise in the Oil and Natural Gas Subsector. Conversely, PSA Program officials said that because of differing perspectives, obtaining information timely from DOE is sometimes challenging. For example, when the program needs to respond to a request for information from DHS leadership, DOE has not had the same urgency to obtain the information. Additional coordination and interaction between the PSA Program and DOE would provide a mutual understanding of similar and competing objectives and perspectives.

DOE officials said both departments work well during emergencies, but NICC information request coordination still needs improvement. For example, in 2009 there was a fire at an oil and natural gas facility in Puerto Rico. As a result, the NICC sent a request for information to DOE and to DHS' Homeland Infrastructure Threat and Risk Analysis Center; the DHS center responded that there were no substantial issues or problems at the facility.[17] DOE, however, responded that the incident could have been serious because of the fuel type handled at the facility. Conflicting assessments made it difficult for the NICC to obtain timely situational awareness of the incident. By designating an information lead for a facility and its interdependencies before an incident, more efficient information exchange and situational awareness reporting can occur.

[17] The Homeland Infrastructure Threat and Risk Analysis Center coordinates with the intelligence community, law enforcement, SSAs, and owner/operators to produce actionable risk-informed products that contain all-hazards warning, threat, and CIKR protection information for federal, state and local, and private sector partners.

### Increased PSA Program Coordination with Oil and Natural Gas SCC Would Enhance Effectiveness

SCCs provide forums for private industry to identify and implement effective information-sharing capabilities; organize and coordinate sector policies; integrate public sector plans with private-sector initiatives; and provide input to the government on sector research and development efforts and requirements. Increased coordination with the Oil and Natural Gas SCC and greater presence at meetings would strengthen stakeholder and PSA Program communication, allow PSAs involvement in strategies outlined in sector specific plans, and increase PSA Program awareness of issues and needs.

Oil and Natural Gas SCC officials said it does not receive enough information from DHS and wants IP leadership to engage the SCC about what the subsector needs from PSAs and DHS. SCC officials said there is also an opportunity for the subsector to help PSAs build necessary public sector relationships and eliminate bottlenecks and misunderstandings. Incorporating the SCC into early program development and planning would facilitate informed exchanges on whether new programs are necessary, or whether existing programs served the same purpose.

Although IP leadership is represented at the SCC meetings through the Partnership and Outreach Division, SCC stakeholders want PSA Program officials more actively engaged. Attending SCC meetings would provide the PSA Program with information about the industry at a local level, which would help bridge potential gaps between program and industry needs. Working more closely with the SCC and SSA would help program management align PSA activities more effectively; understand sector needs and PSA program effects; repair strained relationships; and further DHS goals for developing and sustaining partnerships in all areas of CIKR security.

## Recommendations

We recommend that the Director of the Protective Security Coordination Division:

**Recommendation #5:** Establish formal coordination and collaboration procedures with DOE to facilitate information exchange and ensure that DHS and PSA Program field efforts align and support DOE as the SSA for the Oil and Natural Gas Subsector.

**<u>Recommendation #6:</u>** Establish routine PSA Program leadership involvement in Oil and Natural Gas SCC meetings to obtain Subsector information during project development and to ensure program activities and initiatives align with sector needs and sector specific plans.

## Management Comments and OIG Analysis

**Management Response:** NPPD/IP responded that it non-concurs with Recommendation 5. IP management said that its current efforts meet the intent of this recommendation, as it has formal coordination and collaboration procedures established with all SSAs. IP coordinates directly with all SSAs and at meetings of individual GCCs, the Federal Senior Leadership Council, and their working groups. The PSA Program follows existing procedures to coordinate and collaborate with the SSAs through IP's Partnership and Outreach Division and its Sector-Specific Agency Executive Management Office.

IP responded that in particular, PSCD and PSA Program officials engage DOE to participate in a multitude of efforts. DOE personnel responsible for SSA functions have established relationships and points of contact within PSCD and the PSA Program that afford DOE direct access to rapidly communicate and address issues that may arise. DOE receives briefings and information on PSA efforts, which the PSA program will continue to provide.

As an example of collaboration efforts, IP officials said that the PSA Program is working with all SSAs to calibrate the weights and scores of the ECIP security surveys to address the unique characteristics of each sector. These efforts will enhance the utility of the ECIP surveys and Dashboards to owner/operators by providing a more accurate comparison of similar facilities.

In August 2010, DOE personnel met with PSA Program personnel to adjust ECIP security survey scores and weights to address the unique characteristics of the Energy Sector, its subsectors, segments, and assets. With the assistance of the SSAs, DHS will be able to provide a more complete picture of the current posture of facilities within a sector, as well as across the sectors. The PSA

Program also regularly coordinates with SSAs by providing notification of upcoming ECIP visits, and providing ECIP security survey data.

**OIG Analysis:** We consider IP's current and proposed actions partially responsive to Recommendation 5, which remains resolved and open. The intent of this recommendation is for the PSA Program to establish formal coordination and collaboration procedures with DOE to facilitate information exchange, which IP demonstrated it has done. However, we also recommended that the PSA Program ensure its field efforts align and support DOE as the SSA for the Oil and Natural Gas Subsector. DOE officials said they want to be involved in the assessment programs, but do not have additional dedicated resources to participate in most PSA field assessments and visits. Because DOE is unable to participate in most cases, officials are concerned about PSA interactions with stakeholders and information collected.

Recent efforts by the PSA Program to collaborate and communicate more effectively with DOE and other SSAs on ECIP metrics development are commendable; and DOE acknowledges that communication has improved. This recommendation will remain open pending our receipt of documentation that supports the engagement of and coordination with DOE concerning PSA Program field assessments and visits, and details PSA interactions with Oil and Natural Gas Subsector stakeholders and information collection.

**Management Response:** NPPD/IP concurred with Recommendation 6. IP responded that it has formal coordination and collaboration procedures between it and the SCC through IP's Partnership and Outreach Division, which is the main interaction conduit between the SCCs and IP. IP leadership, including PSA Program management staff, routinely attends Energy Sector and Subsector Critical Infrastructure Partnership Advisory Council meetings and conference calls, when invited, to discuss IP activities. IP leadership also attends Oil and Natural Gas Subsector SCC meetings, when invited, although the SCC has historically preferred to reserve such discussions for the Critical Infrastructure Partnership Advisory Council meetings.

IP's Partnership and Outreach Division will continue to elicit specific concerns and needs of the Oil and Natural Gas Subsector SCC, and ensure such communication to IP and DHS entities, including the PSA Program, to facilitate improved activity coordination and collaboration.  PSCD and the PSA Program will continue to work with critical infrastructure partners, including the SCCs, to ensure that advances in critical infrastructure protection tools and methodologies align with sector-level needs and national priorities.

**OIG Analysis:** We consider IP's proposed actions responsive to Recommendation 6, which remains resolved and open.  Although IP has formal coordination and collaboration procedures between it and the SCC through its Partnership and Outreach Division, incorporating the SCC into early program development and planning would facilitate informed exchanges on whether new programs are necessary, or whether existing programs serve the same purpose.

Establishing routine PSA Program leadership involvement in Oil and Natural Gas SCC meetings to obtain subsector information during project development would ensure PSA Program activities and initiatives align with sector needs and sector specific plans. This recommendation will remain open pending our receipt of documentation that the PSA Program is working routinely with the SCCs, and details program efforts to ensure that advances in critical infrastructure protection tools and methodologies align with sector-level needs and national priorities.

## Current Metrics are Inadequate to Measure PSA Program Performance and Outcomes

As the PSA Program currently uses quantitative metrics to evaluate performance, those metrics only identify the amount of activity carried out by PSAs and do not demonstrate what outcome resulted from conducting assessments.  By developing qualitative measures, the program would be able to assess the value of those activities to stakeholders.  Current quantitative metrics do not consider jurisdictional and sector differences, and as more assessments of CIKR facilities occur, qualitative measures that capture assessment value will become increasingly important. Because interaction with the PSA Program is voluntary and there is no mandatory follow-up, it may be difficult for program officials to determine whether coordination of vulnerability assessments, incident support, and information sharing have improved the security posture of stakeholders.  In addition, because of the nature of risk mitigation, it may be difficult to measure the effect of PSA activity on the Nation's CIKR risk.  However, this is not specific to the PSA Program, and will continue to be a challenge for the sectors and DHS' CIKR efforts overall.

## PSA Performance Metrics Do Not Capture Full Program Effectiveness

The PSA Program currently evaluates its effect through four PSA performance metrics.  All four are quantitative, and based on counting instances of a specific activity carried out by PSAs or supporting staff:

- Outreach visits to partners and facilities, which include working on or planning protection efforts through assessments, exercises, information sharing, or incident response;
- National-level assessments, which include coordinating and working on prevention and protection efforts through training and evaluating strategies;
- Analyses performed on specific threats using vulnerability and consequence information for highly populated cities with a large CIKR concentration; and
- Analyses performed on nationally designated special events to support the Federal Coordinator.

While these dissemination measures are valuable for demonstrating PSA efforts to help facilities and communities reduce exposure, these outputs do not demonstrate specific actions or risk reduction outcomes resulting from those actions.  In addition, the current metrics do not fully capture PSA liaison activities.  A major aspect of a PSA’s usefulness to DHS and stakeholders is the ability to build reliable relationships during events and incidents.  Current metrics count PSA attempts to establish a relationship; they do not measure stakeholder satisfaction with the PSA or measure whether a PSA has become a true stakeholder resource.  The PSA Program can obtain this information by becoming more engaged in SCC meetings and receiving direct feedback from stakeholders.

## Preparedness, Engagement, and Openness Differ Among Sectors

The 18 CIKR sectors differ significantly in nature, scope, engagement in critical infrastructure protection efforts, and NIPP implementation.  Most of the oil and natural gas industry has been securing and protecting its infrastructure for decades because of threats such as vandalism, eco-terrorism, natural disasters, and product theft.

The industry as a whole frequently shares best practices through trade associations and committees, as well as professional organizations that focus on the sector, and numerous regulatory agencies often include security among the areas routinely inspected.

Many other sectors, however, are just beginning to recognize CIKR vulnerabilities and risk levels.  This is an area of opportunity for the PSA Program to build relationships and provide needed services.  However, many facilities, especially if unregulated, are unfamiliar with sharing security details with governmental entities, and may be less likely to engage in a relationship and partnership with the program.  In addition, some industries, even when accustomed to regulation, are extremely reluctant to share information with anyone, especially government entities.  Relationships must be built slowly and deliberately to demonstrate partnership value and necessity for the PSA to progress its risk reduction relationship.  When the PSA Program measures effectiveness quantitatively, there is no opportunity to determine the differences in sector openness, engagement, and levels of preparedness and organization.

## Distribution of CIKR Assets Differ Among Jurisdictions

Some states have high concentrations of critical infrastructure in certain areas.  For example, oil and natural gas industry assets are more predominant in certain states, such as those in the Gulf Coast region.  In some states, such as New Jersey, these assets may be concentrated in close proximity to populated areas or other industries that could pose a threat should disruption occur.  Some states may have three or four critical facilities spread over a large geographic area, while a city in another state may have more than 100 critical assets.  In addition, some cities or states may have large, recurring national level exercises, while in another state the PSA might work on a number of smaller local exercises.  An asset rich location can provide a PSA with many opportunities to engage stakeholders, which stakeholders have described as extremely valuable.  This engagement increases the likelihood of conducting assessments.  The PSA Program measures its effectiveness by PSA performance, and current performance metrics do not account for jurisdiction and geographic differences, which could affect program performance estimates.

### Measuring Program Effect Will Continue to be a Challenge

Challenges in measuring PSA Program risk reduction efforts will continue because stakeholder participation is voluntary, and PSAs have not tracked or recorded recommendation implementation. Although the surveys and ECIP Dashboard inform owner/operators how to further reduce risk, the program has not conducted subsequent assessments at those facilities. These tools provide the facility with a picture of its current protective measure index, but do not account for a comparison of protection levels over time. By increasing coordination and information sharing with the SSAs and other regulatory entities, the PSA Program may be able to obtain data regarding changes in protective measures over time.

In addition, because the PSAs have not conducted multiple ECIPs and SAVs at the same facility, there is the potential for assessment of all critical infrastructure assets in a jurisdiction. Though this may be many years in the future, such an occurrence would diminish quantitative metrics value, and increase the importance of determining stakeholder satisfaction.

According to DHS' Strategic Plan, qualitative and quantitative risk assessments will inform the department's decisions on the use of limited resources, which "will be targeted at the most significant threats, vulnerabilities, and potential consequences."[18] The PSA Program needs to be prepared to measure efforts and activities using quantitative and qualitative metrics where appropriate.

## Recommendation

We recommend that the Director of the Protective Security Coordination Division:

**Recommendation #7:** Define qualitative metrics that account for the extent to which PSA activities contribute to achieving PSA Program, IP, NPPD, and DHS CIKR protection goals and objectives.

[18] *U.S. Department of Homeland Security Strategic Plan Fiscal Years 2008-2013*, September 2008.

## Management Comments and OIG Analysis

**Management Response:** NPPD/IP concurred with Recommendation 7**:** In its response, IP said that the PSA Program has grown and matured since its inception to become a focal point for IP activities and interaction with state, local, tribal and territorial and private sector partners, and DHS as a whole. As such, IP developed new metrics to capture the program's impact on securing the Nation's critical infrastructure. As noted in response to Recommendations 1, PSCD is using 180-day assessment follow-up interviews to capture data on how the PSAs, IP, and NPPD are buying down risk for the Nation's critical infrastructure owner/operators, and demonstrating progress in protecting critical infrastructure.

This implementation data is being used to develop performance metrics for the PSA Program that demonstrate how PSA activities contributed to PSA Program, IP, NPPD, and DHS critical infrastructure protection and resilience goals and objectives, as articulated in the Quadrennial Homeland Security Review and Bottom Up Review.

**OIG Analysis:** We consider IP's proposed actions responsive to Recommendation 7, which remains resolved and open. However, the proposed metrics as described in IP's response suggest outcome-based efforts that align more with guiding programmatic planning and measuring progress toward specific CIKR goals and objectives. Assessing and mitigating CIKR vulnerabilities is only one aspect of the PSA Program's partnership with stakeholders, and metrics based on such data do not capture the less tangible aspects of the program's successes or challenges. The intent of this recommendation is to develop qualitative measures, so that the program would be able to assess the value of those activities to stakeholders.

Because the PSA Program builds relationships, soliciting feedback from public and private sector stakeholders on the quality of their interactions with the PSAs and the value of the program as a DHS resource is key in measuring the program's success. This recommendation remains open pending our receipt of metrics designed to capture qualitative measures, which assess the value of those activities to stakeholders.

# Conclusion

Public and private stakeholders consider the PSA Program an effective resource. Initially focused on establishing local partnerships to increase resilience of CIKR against terrorism, PSA activities have expanded to include all aspects of securing and protecting the nation's CIKR in an all-hazards environment. As more innovative methods, techniques, and tools are developed, the program is adapting accordingly to meet the needs of DHS' partners and to maintain PSA Program staff capabilities. While extensive stakeholder relationships and partnerships are developing at the state, local, and community levels, more attention is necessary to incorporate national level partners and stakeholders into PSA Program strategic planning. Enhanced efforts to coordinate within DHS and to collaborate with federal partners would increase the program's value to stakeholders.

We reviewed how the PSA Program supports DHS' mission to protect the nation's CIKR in the Oil and Natural Gas Subsector of the Energy Sector. We also reviewed the program's role in coordinating with subsector stakeholders to help strengthen critical infrastructure protection capabilities, identify vulnerabilities, and reduce risks. We did not include an evaluation of the Electricity Subsector in this review. Our objectives were to determine:

- to what extent PSAs are aligned to support NPPD's mission and DHS' overall critical infrastructure protection strategy;
- the metrics that the PSA Program uses to assess its own performance;
- whether adequate guidance and resources have been provided to support program growth;
- the methods that PSAs use to coordinate with and assist oil and natural gas stakeholders in identifying, prioritizing, assessing, and protecting critical infrastructure and key resources in this subsector; and
- how oil and natural gas stakeholders use the work performed by PSAs to help strengthen the subsector's critical infrastructure protection capabilities, identify vulnerabilities, and reduce risks.

We reviewed relevant legislation, regulations, directives, policies, strategic plans, annual reports, and collected program documents, including budgets, official guidance documents and manuals, guidelines, operating procedures, and position descriptions. We also studied work previously performed by our office and the Government Accountability Office in this and associated areas.

In Washington, D.C., we interviewed PSA Program officials; other officials within IP's Protective Security Coordination, Infrastructure Information Collection, and Partnership and Outreach Divisions; as well as officials in TSA's Pipeline Security Division. We also interviewed DOE officials from the Office of Fossil Energy and Office of Electricity Delivery and Energy Reliability's Infrastructure Security and Energy Restoration Division.

We conducted fieldwork in locations where we could obtain multiple Oil and Natural Gas Subsector stakeholder perspectives. We visited New Orleans and Baton Rouge, Louisiana; Oklahoma City, Oklahoma; Austin and Dallas, Texas; New York City and

Albany, New York; Trenton, New Jersey; and Sacramento and Los Angeles, California.

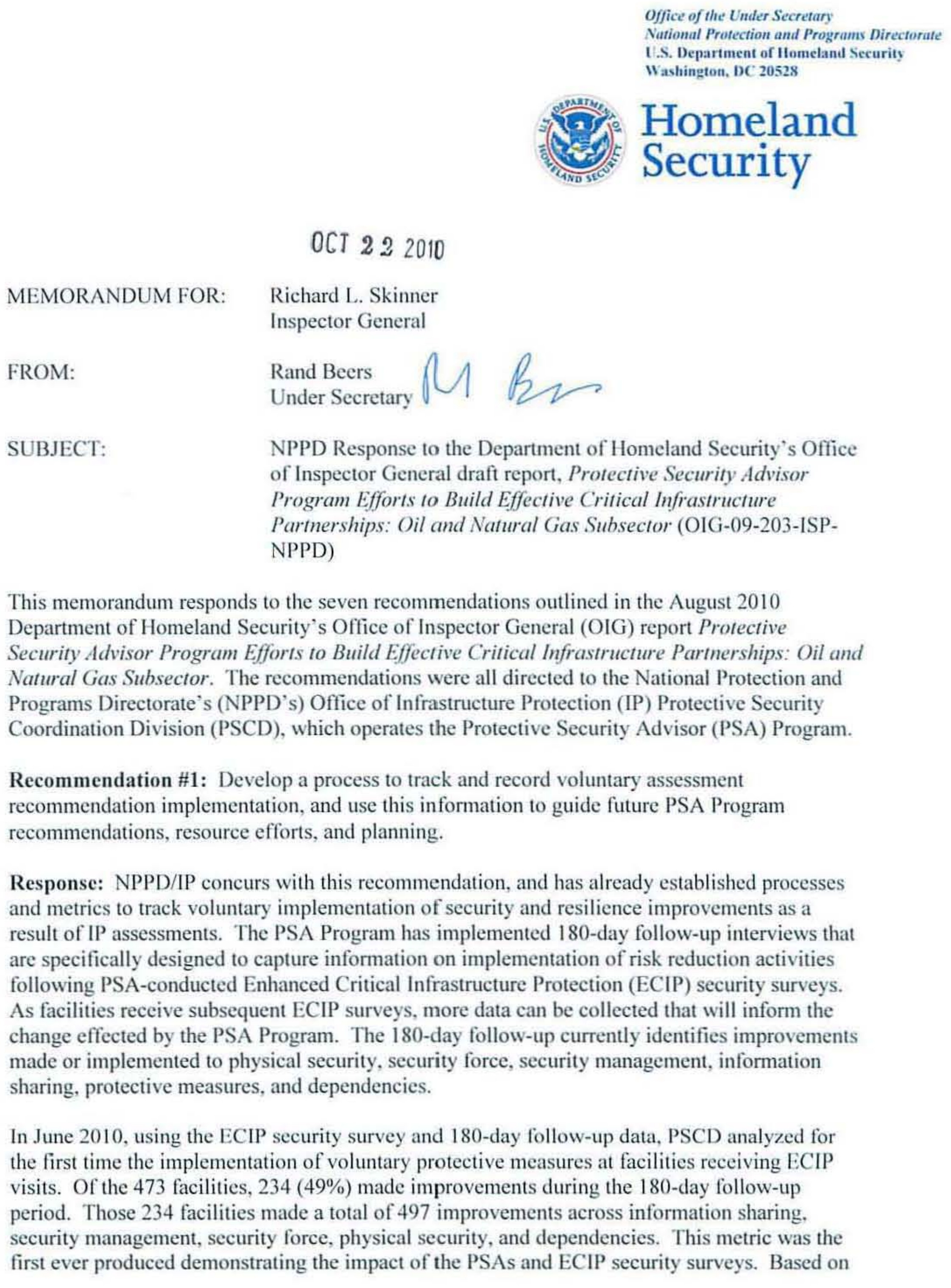
In each state visited, we interviewed PSAs; state and local homeland security and emergency management officials; oil and natural gas industry facility and security managers; and industry and trade association representatives. Our stakeholder sample included officials who had worked with one or more PSAs regularly, periodically, and only a few times. We also spoke with stakeholders who had never worked with a PSA, as well as stakeholders unaware of the PSA Program.

We conducted telephone interviews with stakeholders in Corpus Christi and Houston, Texas; Salt Lake City, Utah; and Washington, D.C. We also interviewed the IP Regional Directors in Atlanta, Georgia and Salt Lake City, Utah, as well as the PSA in Anchorage, Alaska by telephone.

PSAs, state and local emergency management and homeland security officials we interviewed are involved in all 18 CIKR sectors. Therefore, stakeholder perspectives describe PSA work in all sectors represented in specific jurisdictions and districts, although examples provided are specific to the Oil and Natural Gas Subsector.

We performed our fieldwork between November 2009 and April 2010. We initiated this review under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspections*, issued by the President's Council on Integrity and Efficiency.

## Appendix B
## Management Comments to the Draft Report



*Office of the Under Secretary*
*National Protection and Programs Directorate*
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

OCT 22 2010

MEMORANDUM FOR: Richard L. Skinner
Inspector General

FROM: Rand Beers
Under Secretary

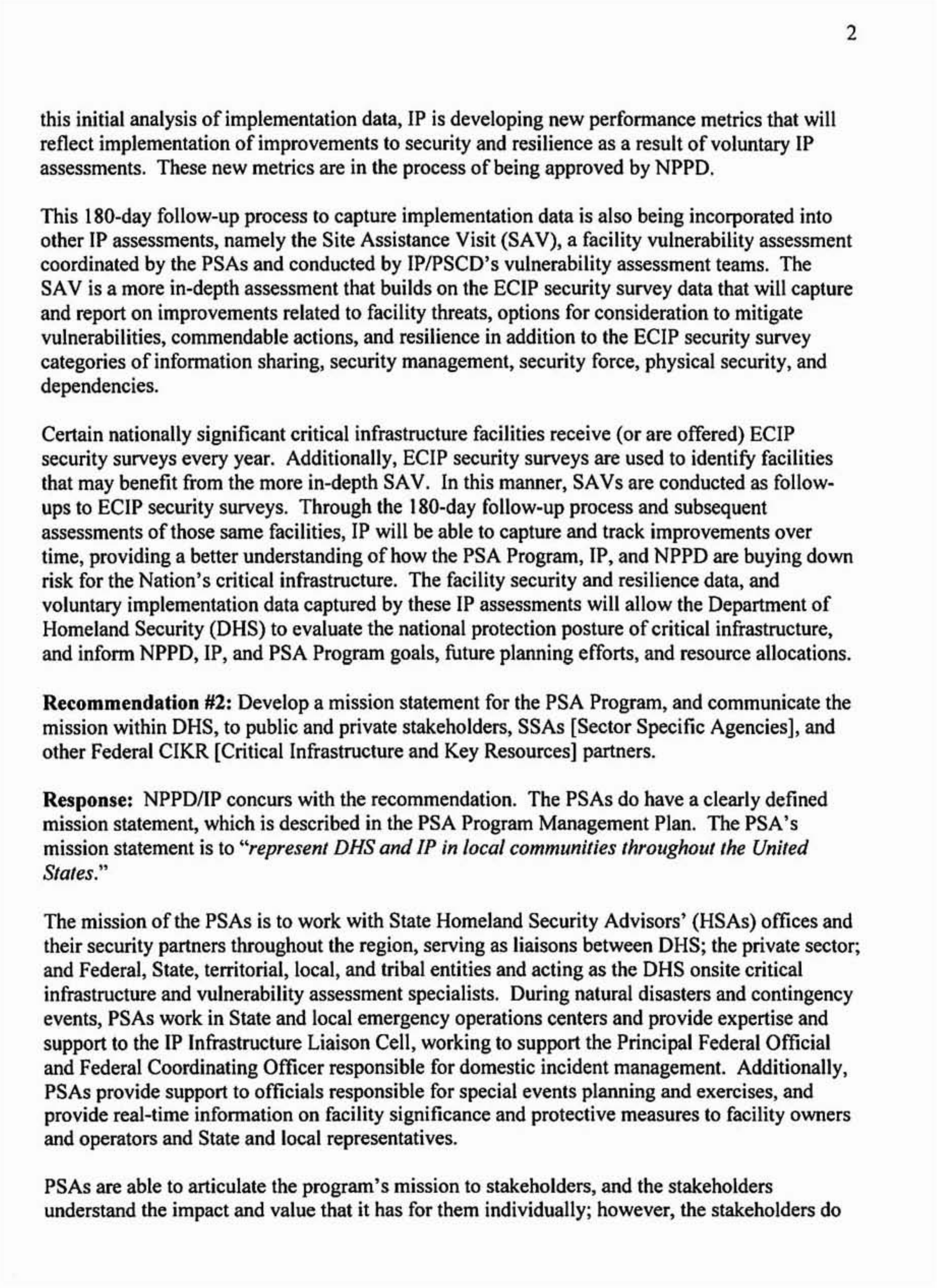
SUBJECT: NPPD Response to the Department of Homeland Security's Office of Inspector General draft report, *Protective Security Advisor Program Efforts to Build Effective Critical Infrastructure Partnerships: Oil and Natural Gas Subsector* (OIG-09-203-ISP-NPPD)

This memorandum responds to the seven recommendations outlined in the August 2010 Department of Homeland Security's Office of Inspector General (OIG) report *Protective Security Advisor Program Efforts to Build Effective Critical Infrastructure Partnerships: Oil and Natural Gas Subsector*. The recommendations were all directed to the National Protection and Programs Directorate's (NPPD's) Office of Infrastructure Protection (IP) Protective Security Coordination Division (PSCD), which operates the Protective Security Advisor (PSA) Program.

**Recommendation #1:** Develop a process to track and record voluntary assessment recommendation implementation, and use this information to guide future PSA Program recommendations, resource efforts, and planning.

**Response:** NPPD/IP concurs with this recommendation, and has already established processes and metrics to track voluntary implementation of security and resilience improvements as a result of IP assessments. The PSA Program has implemented 180-day follow-up interviews that are specifically designed to capture information on implementation of risk reduction activities following PSA-conducted Enhanced Critical Infrastructure Protection (ECIP) security surveys. As facilities receive subsequent ECIP surveys, more data can be collected that will inform the change effected by the PSA Program. The 180-day follow-up currently identifies improvements made or implemented to physical security, security force, security management, information sharing, protective measures, and dependencies.

In June 2010, using the ECIP security survey and 180-day follow-up data, PSCD analyzed for the first time the implementation of voluntary protective measures at facilities receiving ECIP visits. Of the 473 facilities, 234 (49%) made improvements during the 180-day follow-up period. Those 234 facilities made a total of 497 improvements across information sharing, security management, security force, physical security, and dependencies. This metric was the first ever produced demonstrating the impact of the PSAs and ECIP security surveys. Based on



this initial analysis of implementation data, IP is developing new performance metrics that will reflect implementation of improvements to security and resilience as a result of voluntary IP assessments. These new metrics are in the process of being approved by NPPD.

This 180-day follow-up process to capture implementation data is also being incorporated into other IP assessments, namely the Site Assistance Visit (SAV), a facility vulnerability assessment coordinated by the PSAs and conducted by IP/PSCD's vulnerability assessment teams. The SAV is a more in-depth assessment that builds on the ECIP security survey data that will capture and report on improvements related to facility threats, options for consideration to mitigate vulnerabilities, commendable actions, and resilience in addition to the ECIP security survey categories of information sharing, security management, security force, physical security, and dependencies.

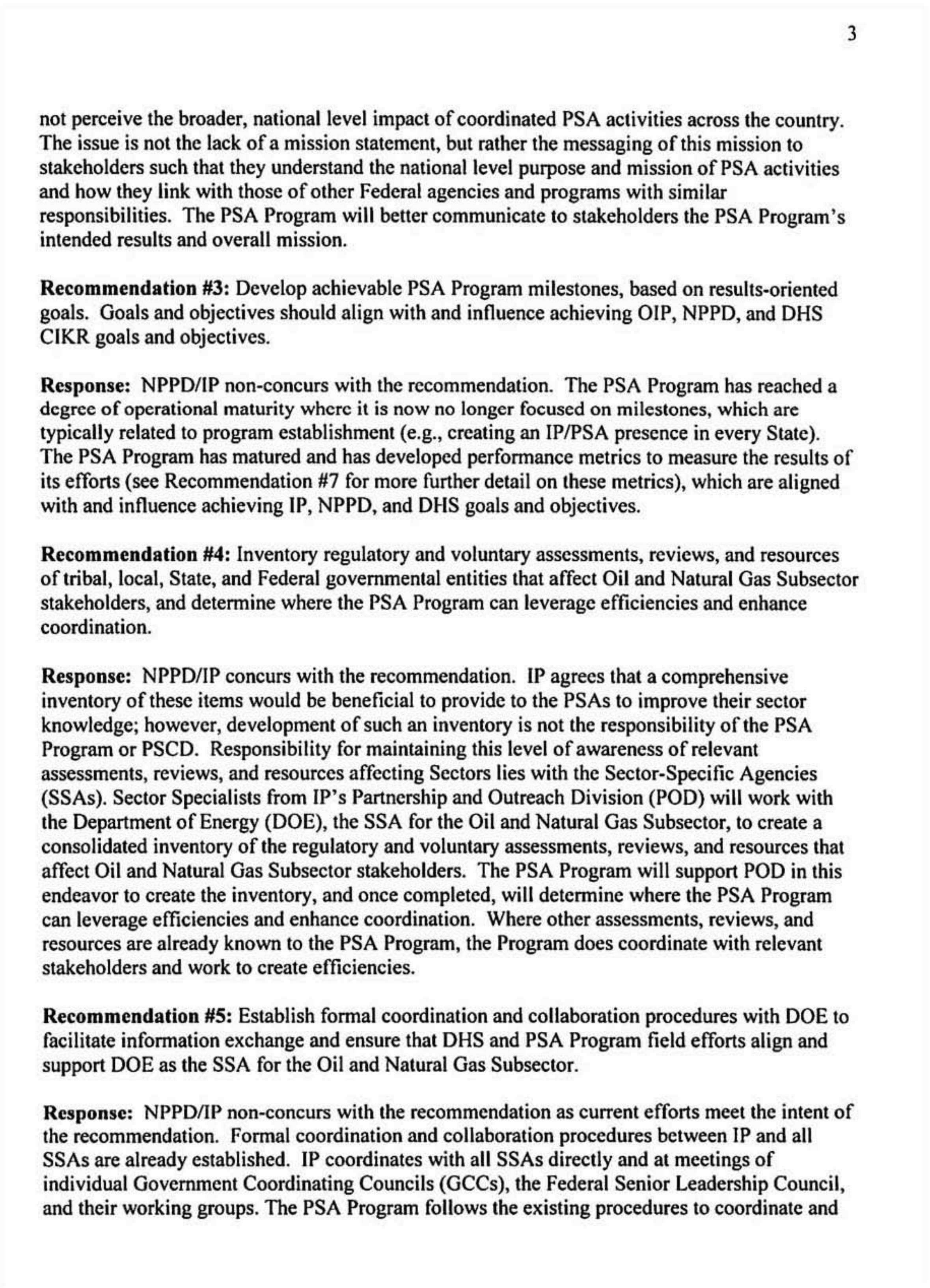
Certain nationally significant critical infrastructure facilities receive (or are offered) ECIP security surveys every year. Additionally, ECIP security surveys are used to identify facilities that may benefit from the more in-depth SAV. In this manner, SAVs are conducted as follow-ups to ECIP security surveys. Through the 180-day follow-up process and subsequent assessments of those same facilities, IP will be able to capture and track improvements over time, providing a better understanding of how the PSA Program, IP, and NPPD are buying down risk for the Nation's critical infrastructure. The facility security and resilience data, and voluntary implementation data captured by these IP assessments will allow the Department of Homeland Security (DHS) to evaluate the national protection posture of critical infrastructure, and inform NPPD, IP, and PSA Program goals, future planning efforts, and resource allocations.

**Recommendation #2:** Develop a mission statement for the PSA Program, and communicate the mission within DHS, to public and private stakeholders, SSAs [Sector Specific Agencies], and other Federal CIKR [Critical Infrastructure and Key Resources] partners.

**Response:** NPPD/IP concurs with the recommendation. The PSAs do have a clearly defined mission statement, which is described in the PSA Program Management Plan. The PSA's mission statement is to "*represent DHS and IP in local communities throughout the United States*."

The mission of the PSAs is to work with State Homeland Security Advisors' (HSAs) offices and their security partners throughout the region, serving as liaisons between DHS; the private sector; and Federal, State, territorial, local, and tribal entities and acting as the DHS onsite critical infrastructure and vulnerability assessment specialists. During natural disasters and contingency events, PSAs work in State and local emergency operations centers and provide expertise and support to the IP Infrastructure Liaison Cell, working to support the Principal Federal Official and Federal Coordinating Officer responsible for domestic incident management. Additionally, PSAs provide support to officials responsible for special events planning and exercises, and provide real-time information on facility significance and protective measures to facility owners and operators and State and local representatives.

PSAs are able to articulate the program's mission to stakeholders, and the stakeholders understand the impact and value that it has for them individually; however, the stakeholders do



not perceive the broader, national level impact of coordinated PSA activities across the country. The issue is not the lack of a mission statement, but rather the messaging of this mission to stakeholders such that they understand the national level purpose and mission of PSA activities and how they link with those of other Federal agencies and programs with similar responsibilities. The PSA Program will better communicate to stakeholders the PSA Program's intended results and overall mission.

**Recommendation #3:** Develop achievable PSA Program milestones, based on results-oriented goals. Goals and objectives should align with and influence achieving OIP, NPPD, and DHS CIKR goals and objectives.

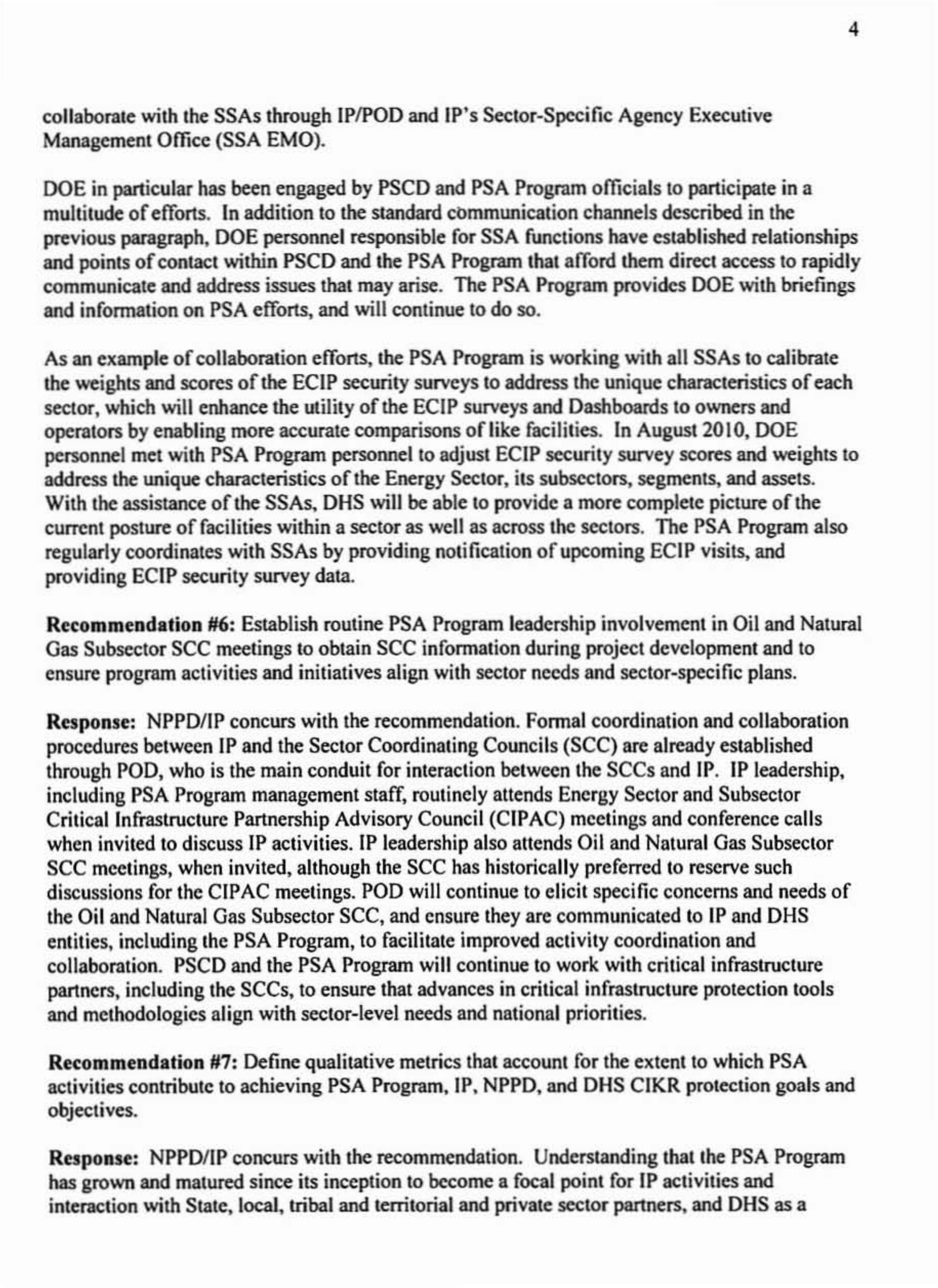
**Response:** NPPD/IP non-concurs with the recommendation. The PSA Program has reached a degree of operational maturity where it is now no longer focused on milestones, which are typically related to program establishment (e.g., creating an IP/PSA presence in every State). The PSA Program has matured and has developed performance metrics to measure the results of its efforts (see Recommendation #7 for more further detail on these metrics), which are aligned with and influence achieving IP, NPPD, and DHS goals and objectives.

**Recommendation #4:** Inventory regulatory and voluntary assessments, reviews, and resources of tribal, local, State, and Federal governmental entities that affect Oil and Natural Gas Subsector stakeholders, and determine where the PSA Program can leverage efficiencies and enhance coordination.

**Response:** NPPD/IP concurs with the recommendation. IP agrees that a comprehensive inventory of these items would be beneficial to provide to the PSAs to improve their sector knowledge; however, development of such an inventory is not the responsibility of the PSA Program or PSCD. Responsibility for maintaining this level of awareness of relevant assessments, reviews, and resources affecting Sectors lies with the Sector-Specific Agencies (SSAs). Sector Specialists from IP's Partnership and Outreach Division (POD) will work with the Department of Energy (DOE), the SSA for the Oil and Natural Gas Subsector, to create a consolidated inventory of the regulatory and voluntary assessments, reviews, and resources that affect Oil and Natural Gas Subsector stakeholders. The PSA Program will support POD in this endeavor to create the inventory, and once completed, will determine where the PSA Program can leverage efficiencies and enhance coordination. Where other assessments, reviews, and resources are already known to the PSA Program, the Program does coordinate with relevant stakeholders and work to create efficiencies.

**Recommendation #5:** Establish formal coordination and collaboration procedures with DOE to facilitate information exchange and ensure that DHS and PSA Program field efforts align and support DOE as the SSA for the Oil and Natural Gas Subsector.

**Response:** NPPD/IP non-concurs with the recommendation as current efforts meet the intent of the recommendation. Formal coordination and collaboration procedures between IP and all SSAs are already established. IP coordinates with all SSAs directly and at meetings of individual Government Coordinating Councils (GCCs), the Federal Senior Leadership Council, and their working groups. The PSA Program follows the existing procedures to coordinate and



collaborate with the SSAs through IP/POD and IP's Sector-Specific Agency Executive Management Office (SSA EMO).

DOE in particular has been engaged by PSCD and PSA Program officials to participate in a multitude of efforts. In addition to the standard communication channels described in the previous paragraph, DOE personnel responsible for SSA functions have established relationships and points of contact within PSCD and the PSA Program that afford them direct access to rapidly communicate and address issues that may arise. The PSA Program provides DOE with briefings and information on PSA efforts, and will continue to do so.

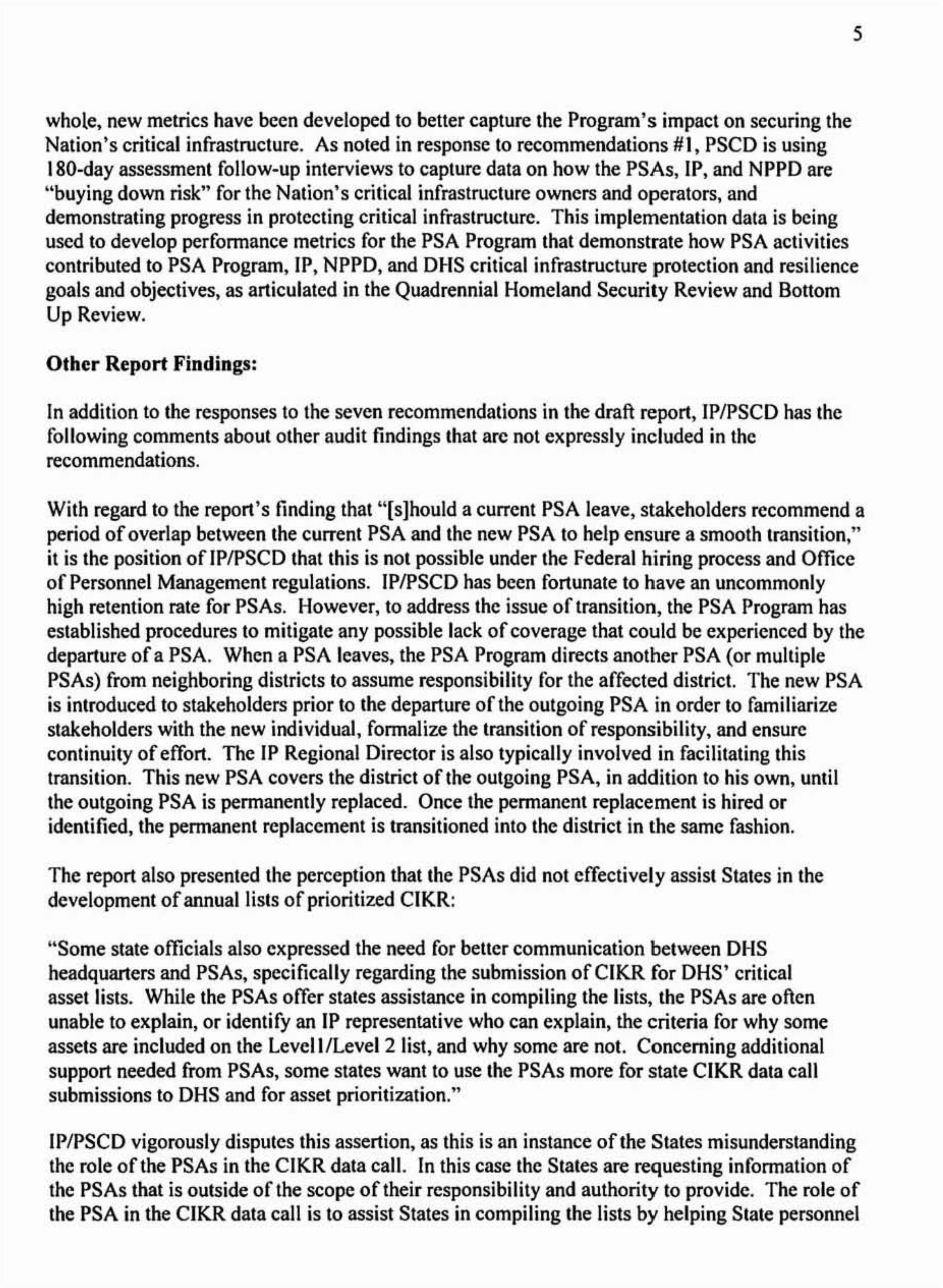
As an example of collaboration efforts, the PSA Program is working with all SSAs to calibrate the weights and scores of the ECIP security surveys to address the unique characteristics of each sector, which will enhance the utility of the ECIP surveys and Dashboards to owners and operators by enabling more accurate comparisons of like facilities. In August 2010, DOE personnel met with PSA Program personnel to adjust ECIP security survey scores and weights to address the unique characteristics of the Energy Sector, its subsectors, segments, and assets. With the assistance of the SSAs, DHS will be able to provide a more complete picture of the current posture of facilities within a sector as well as across the sectors. The PSA Program also regularly coordinates with SSAs by providing notification of upcoming ECIP visits, and providing ECIP security survey data.

**Recommendation #6:** Establish routine PSA Program leadership involvement in Oil and Natural Gas Subsector SCC meetings to obtain SCC information during project development and to ensure program activities and initiatives align with sector needs and sector-specific plans.

**Response:** NPPD/IP concurs with the recommendation. Formal coordination and collaboration procedures between IP and the Sector Coordinating Councils (SCC) are already established through POD, who is the main conduit for interaction between the SCCs and IP. IP leadership, including PSA Program management staff, routinely attends Energy Sector and Subsector Critical Infrastructure Partnership Advisory Council (CIPAC) meetings and conference calls when invited to discuss IP activities. IP leadership also attends Oil and Natural Gas Subsector SCC meetings, when invited, although the SCC has historically preferred to reserve such discussions for the CIPAC meetings. POD will continue to elicit specific concerns and needs of the Oil and Natural Gas Subsector SCC, and ensure they are communicated to IP and DHS entities, including the PSA Program, to facilitate improved activity coordination and collaboration. PSCD and the PSA Program will continue to work with critical infrastructure partners, including the SCCs, to ensure that advances in critical infrastructure protection tools and methodologies align with sector-level needs and national priorities.

**Recommendation #7:** Define qualitative metrics that account for the extent to which PSA activities contribute to achieving PSA Program, IP, NPPD, and DHS CIKR protection goals and objectives.

**Response:** NPPD/IP concurs with the recommendation. Understanding that the PSA Program has grown and matured since its inception to become a focal point for IP activities and interaction with State, local, tribal and territorial and private sector partners, and DHS as a



whole, new metrics have been developed to better capture the Program's impact on securing the Nation's critical infrastructure. As noted in response to recommendations #1, PSCD is using 180-day assessment follow-up interviews to capture data on how the PSAs, IP, and NPPD are "buying down risk" for the Nation's critical infrastructure owners and operators, and demonstrating progress in protecting critical infrastructure. This implementation data is being used to develop performance metrics for the PSA Program that demonstrate how PSA activities contributed to PSA Program, IP, NPPD, and DHS critical infrastructure protection and resilience goals and objectives, as articulated in the Quadrennial Homeland Security Review and Bottom Up Review.

**Other Report Findings:**

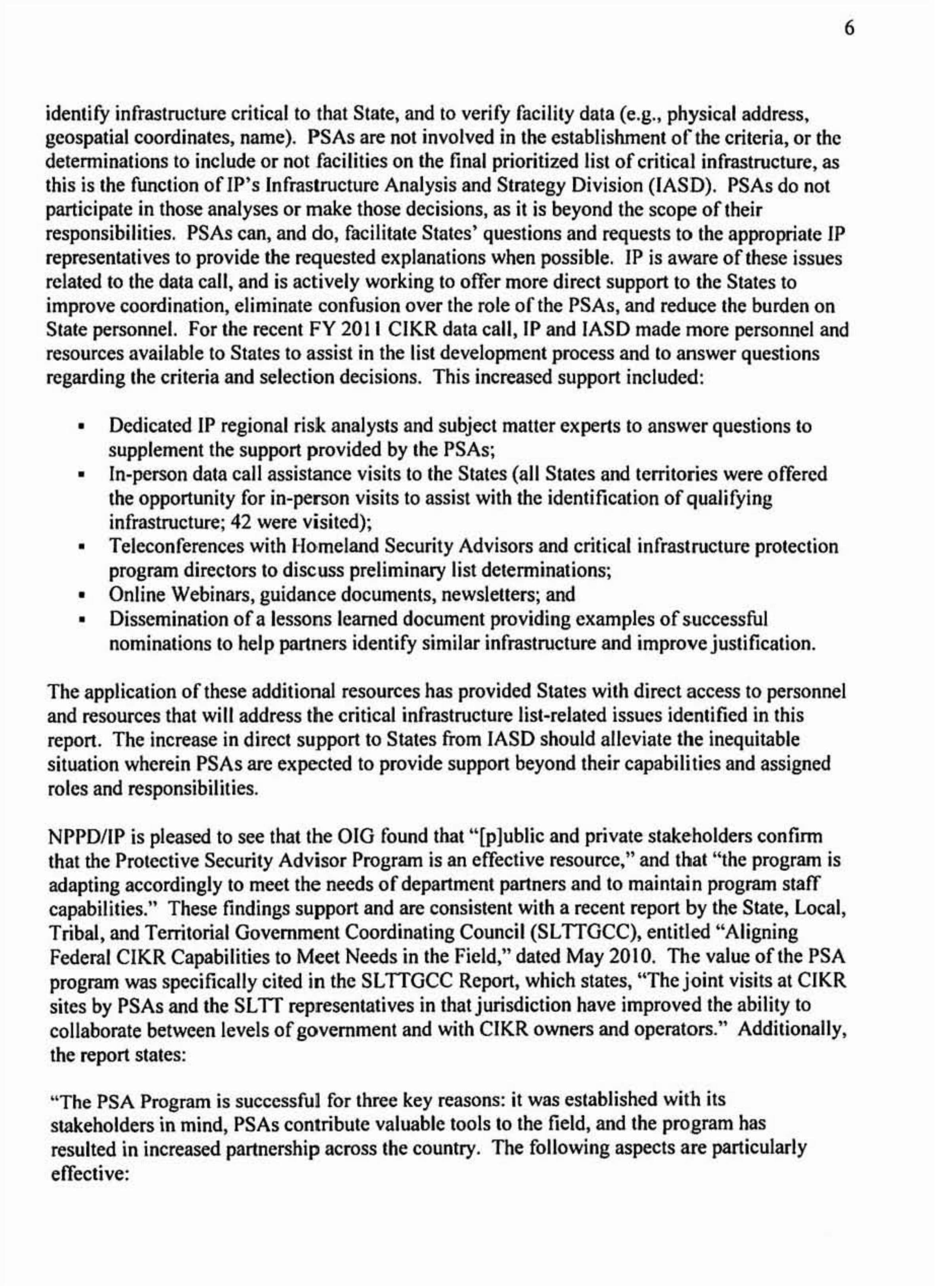
In addition to the responses to the seven recommendations in the draft report, IP/PSCD has the following comments about other audit findings that are not expressly included in the recommendations.

With regard to the report's finding that "[s]hould a current PSA leave, stakeholders recommend a period of overlap between the current PSA and the new PSA to help ensure a smooth transition," it is the position of IP/PSCD that this is not possible under the Federal hiring process and Office of Personnel Management regulations. IP/PSCD has been fortunate to have an uncommonly high retention rate for PSAs. However, to address the issue of transition, the PSA Program has established procedures to mitigate any possible lack of coverage that could be experienced by the departure of a PSA. When a PSA leaves, the PSA Program directs another PSA (or multiple PSAs) from neighboring districts to assume responsibility for the affected district. The new PSA is introduced to stakeholders prior to the departure of the outgoing PSA in order to familiarize stakeholders with the new individual, formalize the transition of responsibility, and ensure continuity of effort. The IP Regional Director is also typically involved in facilitating this transition. This new PSA covers the district of the outgoing PSA, in addition to his own, until the outgoing PSA is permanently replaced. Once the permanent replacement is hired or identified, the permanent replacement is transitioned into the district in the same fashion.

The report also presented the perception that the PSAs did not effectively assist States in the development of annual lists of prioritized CIKR:

"Some state officials also expressed the need for better communication between DHS headquarters and PSAs, specifically regarding the submission of CIKR for DHS' critical asset lists. While the PSAs offer states assistance in compiling the lists, the PSAs are often unable to explain, or identify an IP representative who can explain, the criteria for why some assets are included on the Level1/Level 2 list, and why some are not. Concerning additional support needed from PSAs, some states want to use the PSAs more for state CIKR data call submissions to DHS and for asset prioritization."

IP/PSCD vigorously disputes this assertion, as this is an instance of the States misunderstanding the role of the PSAs in the CIKR data call. In this case the States are requesting information of the PSAs that is outside of the scope of their responsibility and authority to provide. The role of the PSA in the CIKR data call is to assist States in compiling the lists by helping State personnel



identify infrastructure critical to that State, and to verify facility data (e.g., physical address, geospatial coordinates, name). PSAs are not involved in the establishment of the criteria, or the determinations to include or not facilities on the final prioritized list of critical infrastructure, as this is the function of IP's Infrastructure Analysis and Strategy Division (IASD). PSAs do not participate in those analyses or make those decisions, as it is beyond the scope of their responsibilities. PSAs can, and do, facilitate States' questions and requests to the appropriate IP representatives to provide the requested explanations when possible. IP is aware of these issues related to the data call, and is actively working to offer more direct support to the States to improve coordination, eliminate confusion over the role of the PSAs, and reduce the burden on State personnel. For the recent FY 2011 CIKR data call, IP and IASD made more personnel and resources available to States to assist in the list development process and to answer questions regarding the criteria and selection decisions. This increased support included:

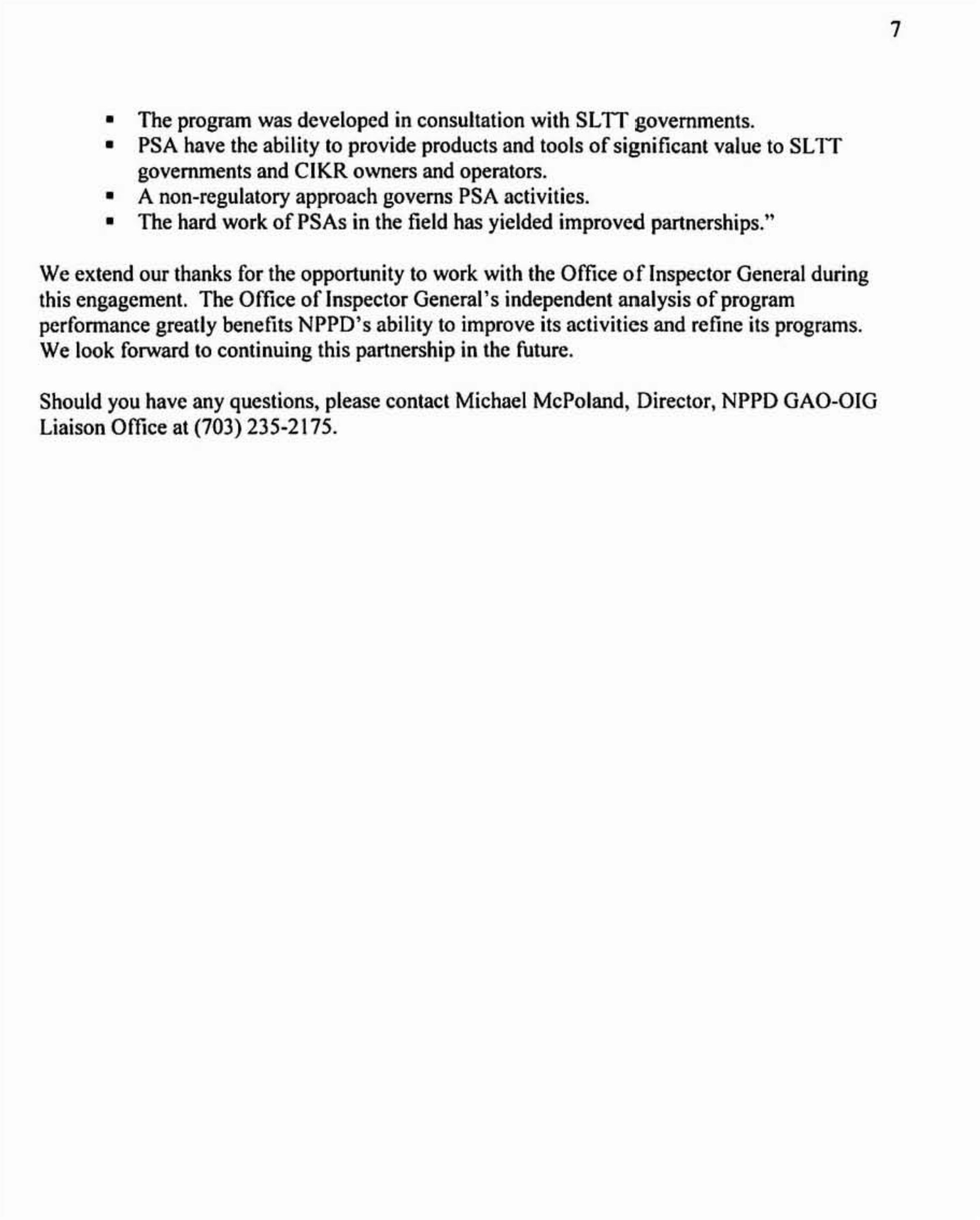
- Dedicated IP regional risk analysts and subject matter experts to answer questions to supplement the support provided by the PSAs;
- In-person data call assistance visits to the States (all States and territories were offered the opportunity for in-person visits to assist with the identification of qualifying infrastructure; 42 were visited);
- Teleconferences with Homeland Security Advisors and critical infrastructure protection program directors to discuss preliminary list determinations;
- Online Webinars, guidance documents, newsletters; and
- Dissemination of a lessons learned document providing examples of successful nominations to help partners identify similar infrastructure and improve justification.

The application of these additional resources has provided States with direct access to personnel and resources that will address the critical infrastructure list-related issues identified in this report. The increase in direct support to States from IASD should alleviate the inequitable situation wherein PSAs are expected to provide support beyond their capabilities and assigned roles and responsibilities.

NPPD/IP is pleased to see that the OIG found that "[p]ublic and private stakeholders confirm that the Protective Security Advisor Program is an effective resource," and that "the program is adapting accordingly to meet the needs of department partners and to maintain program staff capabilities." These findings support and are consistent with a recent report by the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), entitled "Aligning Federal CIKR Capabilities to Meet Needs in the Field," dated May 2010. The value of the PSA program was specifically cited in the SLTTGCC Report, which states, "The joint visits at CIKR sites by PSAs and the SLTT representatives in that jurisdiction have improved the ability to collaborate between levels of government and with CIKR owners and operators." Additionally, the report states:

"The PSA Program is successful for three key reasons: it was established with its stakeholders in mind, PSAs contribute valuable tools to the field, and the program has resulted in increased partnership across the country. The following aspects are particularly effective:

## Appendix B
## Management Comments to the Draft Report



- The program was developed in consultation with SLTT governments.
- PSA have the ability to provide products and tools of significant value to SLTT governments and CIKR owners and operators.
- A non-regulatory approach governs PSA activities.
- The hard work of PSAs in the field has yielded improved partnerships."

We extend our thanks for the opportunity to work with the Office of Inspector General during this engagement. The Office of Inspector General's independent analysis of program performance greatly benefits NPPD's ability to improve its activities and refine its programs. We look forward to continuing this partnership in the future.

Should you have any questions, please contact Michael McPoland, Director, NPPD GAO-OIG Liaison Office at (703) 235-2175.

# Appendix C
# Sectors, Subsectors, and Sector-Specific Agencies

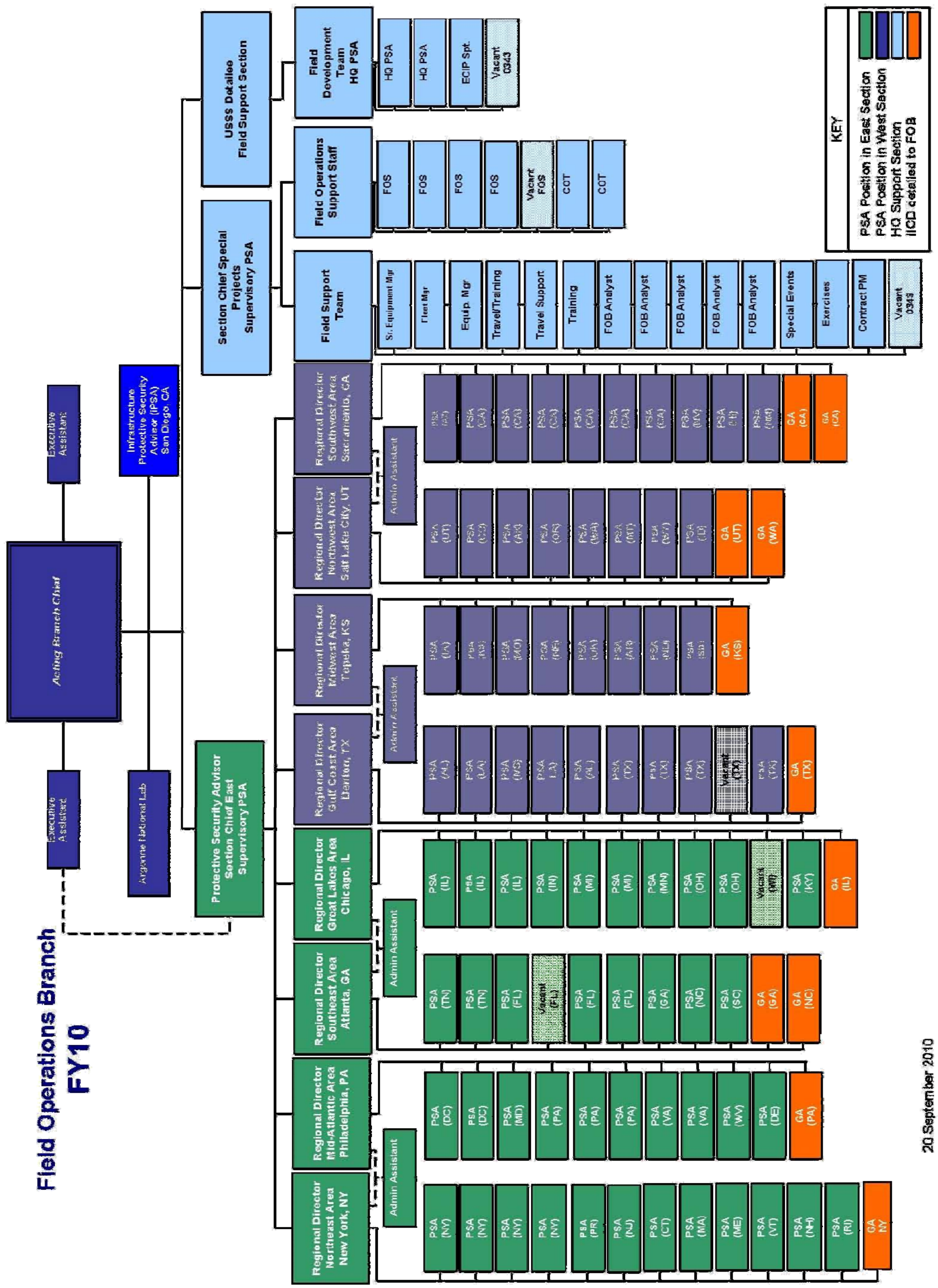
| CIKR Sector (Subsector) | Sector-Specific Agency | Profile |
|---|---|---|
| **Banking and Finance** | Department of the Treasury | Financial institutions including banks, insurers, securities brokers/dealers, and investment companies |
| **Chemical**<br>• Basic Chemicals<br>• Specialty Chemicals<br>• Agricultural Chemicals<br>• Pharmaceuticals<br>• Consumer Products | DHS/Office of Infrastructure Protection | Facilities converting raw materials into chemical products, or using, storing, packaging, transporting, delivering, marketing, recycling, and disposing of the chemicals; including manufacturing plants, transport systems, distribution systems (storage, stockpile, and supply areas), and research and educational institutions |
| **Commercial Facilities**<br>• Real Estate<br>• Public Assembly<br>• Sports Leagues<br>• Gaming<br>• Lodging<br>• Outdoor Events<br>• Entertainment & Media<br>• Retail | DHS/Office of Infrastructure Protection | Office/apartment buildings, condominiums, mixed-use facilities, self-storage<br>Arenas, stadiums, aquariums, zoos, museums, convention centers<br>Professional sports leagues and federations<br>Casinos<br>Hotels, motels, conference centers<br>Theme and amusement parks, fairs, campgrounds, parades<br>Motion picture studios, broadcast media<br>Retail centers and districts, shopping malls |
| **Communications** | DHS/Office of Cybersecurity & Communications | Broadcasting, cable, wireline industries, and networks supporting the Internet; using terrestrial, satellite, and wireless transmission systems |
| **Critical Manufacturing**<br>• Primary Metal<br>• Machinery<br>• Electrical Equipment<br>• Appliances & Components<br>• Transportation Equipment | DHS/Office of Infrastructure Protection | Facilities producing, processing, or converting:<br>Iron, steel, ferro alloys, and aluminum<br>Engines, turbines, and generators<br>Electrical transformers<br>Motors, switchboard apparatus, relays, and industrial controls<br>Motor vehicles, aerospace products, and railroad rolling stock |
| **Dams** | DHS/Office of Infrastructure Protection | Water retention and/or control facilities, including dams, hydropower plants, navigation locks, levees, hurricane barriers, and industrial waste impoundments |
| **Defense Industrial Base** | Department of Defense | Entities performing military-related work, including researching, developing, designing, producing, delivering, and maintaining military weapons systems, subsystems, components, or parts |
| **Emergency Services** | DHS/Office of Infrastructure Protection | System of elements for saving lives, protecting property and the environment, assisting communities impacted by disasters (natural or malevolent), and aiding recovery from emergency situations<br>*[Primary protector for all other CIKR]* |
| **Energy**<br>• Electricity<br>• Oil & Natural Gas | Department of Energy | Generation, transmission, and distribution of electric power, except for commercial nuclear power facilities<br>Production, refining, storage, and distribution of oil and natural gas |

# Appendix C
# Sectors, Subsectors, and Sector-Specific Agencies

| CIKR Sector (Subsector) | Sector-Specific Agency | Profile |
|---|---|---|
| **Food and Agriculture**<br>• Producers/Plant<br>• Producers/Animal<br>• Processors/Manufacturers<br>• Restaurant/Food Service<br>• Retail<br>• Warehousing/Logistics<br>• Agricultural Production Inputs & Services | Department of Agriculture - (Meat, poultry, and egg products; production agriculture)<br>Food & Drug Administration - (Food other than meat, poultry, and egg products; food safety and defense) | Network of systems of production, processing, and delivery including privately owned farms, ranches, and groves; livestock transport areas, and slaughterhouses; crop production and food processing facilities; supply chains for feed, animals, seed, and fertilizers; institutional food services, and grocery stores; domestic and imported food supply safety programs; food assistance programs, and food distribution mechanisms (transportation and warehouses) |
| **Government Facilities**<br>• Educational Facilities | DHS/Federal Protective Service<br>Department of Education - (Educational Facilities) | Buildings owned or leased by Federal, state, territorial, local, or tribal governments, including office buildings, embassies, courthouses, and national laboratories<br>All public and private K-12 schools; public and private higher education institutions, and vocational and trade schools |
| **Healthcare and Public Health** | Department of Health & Human Services | Network of systems to prevent disease and disability, treat patients, foster public health, and respond to public health emergencies including hospitals, laboratories, blood banks, and medical supply manufacturing and distribution |
| **Information Technology** | DHS/Office of Cybersecurity & Communications | Virtual and distributed functions producing and providing hardware, software, IT systems and services, and the Internet |
| **National Monuments and Icons** | Department of the Interior | Monuments, physical structures, or sites widely recognized to represent the nation's heritage, traditions, or values, or of important national cultural, religious, historical, or political significance |
| **Nuclear** | DHS/Office of Infrastructure Protection | Commercial nuclear power plants; nuclear and radiological materials used in medical, industrial, and academic settings; and the transportation, storage, and disposal of nuclear materials and radioactive waste |
| **Postal and Shipping** | DHS/Transportation Security Administration | Providers receiving, processing, transporting, and distributing letters and parcels, including high-volume automated processing facilities; collection, acceptance, and retail operations; courier services; chartered air delivery services; and information and communications networks |
| **Transportation Systems**<br>• Aviation<br>• Freight Rail<br>• Highway<br>• Mass Transit<br>• Maritime<br>• Pipeline | Department of Transportation<br>DHS/U.S. Coast Guard - (Maritime)<br>DHS/Transportation Security Administration - (Pipeline) | Aircraft, commercial airports, and heliports<br>Railroads, track, freight cars, and locomotives<br>Roadways, signature bridges, and tunnels<br>Transit buses, trolleybuses, ferryboats, subways, light rail, and cable cars<br>Water-faring vessels, coastline, ports, navigable waterways, and intermodal landside connections<br>Networks of natural gas, hazardous liquids, and chemical pipelines |
| **Water** | Environmental Protection Agency | Public drinking water systems and wastewater systems (sanitary sewage treatment) |

*Sources: National Infrastructure Protection Plan, February 2009; 2009 Critical Infrastructure Partnership Advisory Council Annual Report; The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003; DHS CIKR Resource Center (http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/sectorMenu.htm, accessed 4/24/10).*

# Appendix D
# PSA Program Organization Chart



*Source: Field Operations Branch, Protective Security Coordination Division, DHS Office of Infrastructure Protection, September 2010.*

## Appendix E
## Energy Government Coordinating Council Membership

U.S. Department of Energy
- Bonneville Power Administration
- Office of Fossil Energy
- Office of Electricity Delivery and Energy Reliability, Office of Infrastructure Security and Energy Restoration

U.S. Department of Homeland Security
- National Cyber Security Division
- National Infrastructure Protection Plan Program Management Office
- Office of Infrastructure Protection
- Office of Infrastructure Protection, Sector Specific Agency Executive Management Office, Chemical Branch
- Office of Infrastructure Protection, Sector Specific Agency Executive Management Office, Dams Branch
- Science & Technology Directorate
- Transportation Security Administration
- Transportation Security Administration, Pipeline Security Division
- U.S. Coast Guard

Environmental Protection Agency
Federal Bureau of Investigation
Federal Energy Regulatory Commission
National Association of Regulatory Utility Commissioners
National Association of State Energy Officials
Natural Resources Canada
State, Local, Tribal, and Territorial Government Coordinating Council
Tennessee Valley Authority
U.S. Army Corps of Engineers
U.S. Committee on the Marine Transportation System
U.S. Department of Agriculture
U.S. Department of Defense
U.S. Department of the Interior, Minerals Management Service
U.S. Department of the Treasury
U.S. Department of Transportation
- Maritime Administration
- Pipeline and Hazardous Materials Safety Administration

Western Area Power Administration

## Appendix F
## Oil and Natural Gas Sector Coordinating Council Membership

AGL Resources, Inc.
American Exploration & Production Council
American Gas Association
American Petroleum Institute
American Public Gas Association
Anadarko Petroleum Corporation
Apache Corporation
Association of Oil Pipe Lines
BP
Canadian Association of Petroleum Producers
Canadian Energy Pipeline Association
Center for Liquified Natural Gas
Collier, Shannon, Scott
Colonial Pipeline
ConocoPhillips
Dominion Resources, Inc.
Duke Energy
Edison Chouest Offshore, LLC
Enbridge
Energy Security Council
ExxonMobil
Flint Hills Resources
Gas Processors Association
Genesis Energy, Inc.
Independent Petroleum Association of America
International Association of Drilling Contractors
International Liquid Terminals Association
Interstate Natural Gas Association of America
Kinder-Morgan Pipelines
Leffler Energy
Marathon Petroleum Company
MSW Consulting, LLC
National Association of Convenience Stores
National Ocean Industries Association
National Petrochemical & Refiners Association
National Propane Gas Association
Nella Oil
NiSource, Inc.
Noble Drilling Services, Inc.
Offshore Marine Service Association
Offshore Operators Committee
Petroleum Fuel & Terminal Company
Petroleum Marketers Association of America
Questar Gas Company

## Appendix F
## Oil and Natural Gas Sector Coordinating Council Membership

Rowan Companies, Inc.
Sempra Energy
Society of Independent Gas Marketers Association
Spectra Energy
Suncor Energy
U.S. Oil & Gas Association
Western States Petroleum Association
Williams Energy

# Appendix G
# Major Contributors to This Report

Marcia Moxey Hodges, Chief Inspector, Department of Homeland Security, Office of Inspector General, Office of Inspections

Katherine Roberts, Team Leader, Department of Homeland Security, Office of Inspector General, Office of Inspections

Kimberley Lake, Inspector, Department of Homeland Security, Office of Inspector General, Office of Inspections

Amy Tomlinson, Inspector, Department of Homeland Security, Office of Inspector General, Office of Inspections

## Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for National Protection and Programs Directorate
Assistant Secretary for Infrastructure Protection
NPPD Audit Liaison
IP Audit Liaison
Director of Local Affairs, Office of Intergovernmental Affairs

## Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

## Congress

Congressional Oversight and Appropriations Committees, as appropriate

## ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

## OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;

- Fax the complaint directly to us at (202) 254-4292;

- Email us at DHSOIGHOTLINE@dhs.gov; or

- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.