



# Strategic Plan on Infrastructure Protection Assessments

October 25, 2017

Fiscal Year 2016 Report to Congress



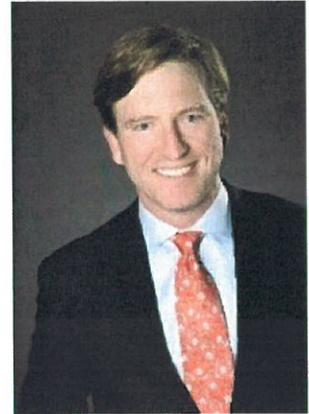
Homeland  
Security

*National Protection and Programs Directorate*

# Message from the Office of the Under Secretary

October 25, 2017

I am pleased to present the following report, “Strategic Plan on Infrastructure Protection Assessments,” which has been prepared by the Office of Infrastructure Protection (IP) in the National Protection and Programs Directorate (NPPD).



This report was compiled in response to language in the Joint Explanatory Statement and Senate Report 114-68, which accompany the Fiscal Year 2016 Department of Homeland Security (DHS) Appropriations Act (P.L. 114-113). IP conducts voluntary security assessments and analyses of the Nation’s critical infrastructure. These assessments are important elements to accomplish the overall NPPD mission to secure and enhance the resilience of the Nation’s cyber and physical infrastructure. NPPD looks forward to continuing to work with Congress as well as the public- and private-sector stakeholders to continue improving voluntary assessments.

In accordance with congressional requirements, this report is being provided to the following Members of Congress:

The Honorable John R. Carter  
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Lucille Roybal-Allard  
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable John Boozman  
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable Jon Tester  
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

If you have any questions, please do not hesitate to contact me at (202) 282-8260 or the Department’s Acting Chief Financial Officer, Stacy Marcott, at (202) 447-5751.

Sincerely,

A handwritten signature in blue ink, appearing to read "Chris Krebs", written over a light blue horizontal line.

Christopher C. Krebs  
Senior Official Performing the Duties of the Under Secretary  
and Assistant Secretary, Office of Infrastructure Protection  
National Protection and Programs Directorate

# Executive Summary

DHS NPPD conducts voluntary security assessments and analyses of the Nation’s critical infrastructure<sup>1</sup>. Within NPPD, IP carries out assessments, supported by Office of Cyber and Infrastructure Analysis (OCIA) analyses, both of which support risk-informed decision-making by critical infrastructure owners and operators, as well as federal, state, local, tribal, and territorial partners. These initiatives address objectives in homeland security legislation, policy, and doctrine, including the *National Infrastructure Protection Plan*.

To develop the 3-year strategic plan for assessments, NPPD assessed the current or “as-is” state of the assessment program by evaluating maturity across five program domains, defined a desired “to-be” state for program maturity, and identified goals and objectives for closing gaps between the current and desired states. This work was informed by extensive engagement with key stakeholders, including interviews with nearly 100 partners, as well as three planning workshops. The resulting 3-year strategic plan enables NPPD to transition the assessment program into a more mature phase that operates with a clearly defined vision or strategic intent, and that better supports data needs for analyses.

NPPD envisions that the voluntary assessments that IP conducts will improve risk management locally, and, when integrated with a body of infrastructure analysis, will enhance the Federal Government’s ability to manage infrastructure risk nationally. Improvements to assessments are intended to achieve the following strategic outcomes:

- Increase the value of DHS voluntary assessments to the critical infrastructure community;
- Clarify opportunities for collaboration and mutual support between IP assessments and OCIA analyses;
- Improve the way that DHS prioritizes and conducts assessments; and
- Strengthen the connections between DHS assessments and critical infrastructure partners, particularly the Federal Emergency Management Agency and other federal partners.

The strategic intent and approach for the assessment program over the next 3 years will increase the comprehensiveness of the national approach to infrastructure risk management, building beyond the identification and securing of critical assets. This strategic plan serves as the foundation for identifying and prioritizing further steps toward achieving national infrastructure risk management goals through adjustments to the assessment program.

---

<sup>1</sup> Within NPPD, voluntary assessments are conducted by IP and the Office of Cybersecurity and Communications. On the basis of the congressional requirement, this strategic plan generally is limited to voluntary assessments carried out by IP.



# Strategic Plan on Infrastructure Protection Assessments

## Table of Contents

|      |   |    |
|------|---|----|
| I.   | Legislative Language.....   | 1  |
| II.  | Background.....   | 2  |
|      | Purpose.....  | 3  |
| III. | Three-Year Strategic Plan.....  | 4  |
|      | Development of the Plan.....  | 5  |
|      | “As-is” State .....   | 5  |
|      | “To-be” State .....   | 6  |
|      | Closing the Gap .....   | 6  |
|      | Strategic Framework: The Voluntary Assessments Maturity Model .....         | 7  |
|      | The Approach to, and Benefits of, a Maturity Model.....                     | 7  |
|      | Developing the Model .....  | 7  |
| IV.  | The Future State: Goals, Objectives, and Metrics .....                      | 10 |
| V.   | Implementation .....  | 13 |
|      | Governance .....  | 13 |
|      | Execution .....   | 13 |
|      | Prioritizing Voluntary Assessments.....                                     | 15 |
|      | Challenges and Opportunities.....   | 16 |
|      | Challenges.....   | 16 |
|      | Opportunities .....   | 17 |
| VI.  | Conclusion .....  | 18 |
|      | Appendices.....   | 19 |
|      | Appendix A: Suite of IP Voluntary Assessments, Analyses, and Programs ..... | 19 |
|      | Appendix B: The Current State: Findings and Stakeholder Needs .....         | 20 |
|      | Domain 1: Fitting Assessments to User Needs.....                            | 20 |

|  |    |
|--|----|
| Domain 2: Conducting Assessments .....           | 24 |
| Domain 3: Managing Assessment Information .....  | 27 |
| Domain 4: Creating Analytic Products .....       | 29 |
| Domain 5: Managing Data Quality.....             | 31 |
| Appendix C: The Strategic Planning Process ..... | 33 |

# I. Legislative Language

This document has been compiled in response to language in the Joint Explanatory Statement and Senate Report 114-68, which accompany the Fiscal Year (FY) 2016 Department of Homeland Security (DHS) Appropriations act (P.L. 114-113).

The Joint Explanatory Statement includes the following requirement.

As described in the Senate report, \$1,500,000 is provided above the request for the Office of Infrastructure Protection and the Office of Cyber Infrastructure and Analysis to develop and submit a three-year strategic plan to guide vulnerability assessments, analytic assessments, and the Regional Resiliency Assessment Program. The plan will guide this suite of programs with a focus on comprehensive assessments of critical lifeline infrastructure dependencies and interdependencies, assisting FEMA in risk assessments that support grant allocation decisions, and enhancing state and local preparedness and resiliency. Included shall be a set of performance metrics against which effectiveness can be measured and reported to Congress on an annual basis.

Senate Report 114-68 states:

## REGIONAL RESILIENCY AND INTERDEPENDENCY ASSESSMENTS

Through the Infrastructure Analysis and Planning PPA, NPPD manages a suite of assessment programs including analytic assessments, vulnerability assessments, and the Regional Resiliency Assessment Program [RRAP]. Together, the three programs offer an assessment of critical infrastructure and examine vulnerabilities, threats, and potential consequences from an all-hazards perspective to identify dependencies, interdependencies, cascading effects, resilience characteristics, and gaps.

To date, these programs have achieved encouraging results, yet the Committee believes improvements can be gained through a better-defined strategic focus and vision. Such analysis can aid in project selection, a risk-based application of funding, and demonstration of measurable risk reduction through quantifiable performance metrics. Therefore, the Committee includes an additional \$1,500,000 and directs IP to develop and submit a 3-year strategic plan that will guide this suite of programs with a specific, priority focus on completing comprehensive assessments of critical lifeline infrastructure dependencies and interdependencies; how to assist FEMA in planning assumptions and support grant allocations including development of the Threat Hazard Identification and Risk Assessments [THIRA]; and enhance the ability of State and local officials to understand and address the physical consequences of a cyber-event. The plan shall outline a process by which IP will conduct a comprehensive assessment in at least 10 of the Urban Area Security Initiative regions. This strategic plan shall include a detailed set of performance metrics against which program effectiveness can be measured and reported to Congress on an annual basis. As recommended funds remain available, IP is encouraged to begin the assessment process.

## II. Background

The Nation's critical infrastructure provides the essential services that underpin American society, national security, economic stability, and public health and safety. Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience and the *National Infrastructure Protection Plan* (NIPP) outline relationships and mechanisms through which the government and private sector act to improve security and resilience of critical infrastructure. In the face of risk posed by threats and hazards such as cyberattack, terrorism, aging infrastructure, and increased frequency of extreme weather events, the DHS Quadrennial Homeland Security Review of 2014 identifies strengthening the security and resilience of critical infrastructure as a key activity of the Department's strategic approach. The continued enhancement of information used to clarify critical infrastructure partners' understanding of threats, vulnerabilities, and consequences, as well as risk-informed decision-making, is an essential part of this aim.

***"[C]ritical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.***

*Critical Infrastructures Protection Act of 2001*

Within the National Protection and Programs Directorate (NPPD), the Office of Infrastructure Protection (IP) is responsible for conducting and facilitating assessments of the Nation's critical infrastructure. To accomplish this activity, IP manages a suite of voluntary security and vulnerability assessments, analytic assessments, and programs to assist critical infrastructure owners and operators, as well as federal and state, local, tribal, and territorial (SLTT) partners, in understanding and addressing risks to critical infrastructure. DHS Protective Security Advisors (PSA) provide voluntary security and vulnerability assessments of facilities and assets. The Office of Cyber and Infrastructure Analysis (OCIA) is responsible for analysis that responds to both government and external stakeholders' needs to understand the consequences of terrorist and cyber attacks, and other disruptions to critical infrastructure. OCIA complements IP's assessments through analysis and studies that support some of IP's programs, and addresses analytic questions that the assessments do not tackle.

IP assessments started in 2004 as a means of identifying vulnerabilities and enhancing the security of critical infrastructure in order to support priorities in the NIPP, the *National Response Plan*, and Homeland Security Presidential Directive 7. When the assessments began, infrastructure protection focused primarily on physical security and combatting terrorism. Over time, this approach has expanded to include a more diverse group of partners across the Federal Government, SLTT agencies, and the private sector. Concurrently, the focus of assessments evolved from an asset-level focus on terrorism to utilizing an all-hazards, regional, and systems approach that extends to infrastructure resilience. This broader approach was coupled with a shift in how information is shared: early assessments were classified, restricting their use to the Federal Government and the security manager at the facility; many current assessments are

designated as Protected Critical Infrastructure Information, which makes it possible to protect information as necessary, while still being able to share reports and analysis with key partners. This cooperative approach has expanded the suite of assessments to customize assessment options better to match stakeholder needs. In 2008, assessments were limited to site assistance visits, comprehensive reviews, and the assessments that supported the Buffer Zone Protection Program. By 2014, these assessments had incorporated a scalable methodology and tracking system to build assessment capacity at all levels of government throughout the Nation. In 2017, IP formalized its approach by establishing this 3-year strategy for assessments.

As NPPD evolves its assessments to incorporate emerging stakeholder requirements and to reflect a shifting risk environment, there is a need to reach a new future state that is more efficient, is more effective, and better meets stakeholder needs. The vision for assessments and analyses is also its strategic intent—*every assessment will improve risk management locally and, when integrated with a body of infrastructure analysis, will enhance the Federal Government’s ability to manage infrastructure risk nationally*. This vision will ensure that assessments operate under a shared set of priorities that supports stakeholder needs and maximizes the Federal Government’s ability to leverage data collected through assessments to improve national security and support public- and private-sector partners.

## Purpose

In alignment with congressional direction, NPPD has developed a 3-year strategic plan for voluntary assessments that reflects the relationship between the assessment program, OCIA’s analysis, and other key capabilities. Through the strategic planning process, IP has defined an approach for how it will enhance the value and impact of its suite of assessments for its stakeholders, and how it will make improvements, address capability gaps, and implement ongoing changes to assessments. This 3-year strategy and plan for assessments will enhance the common scheme for assessment prioritization; will strengthen the connection between risk analysis and assessments; and will support homeland security partners, including with national preparedness efforts and grant-making decisions. Specifically, this plan:

- Articulates the strategic intent of assessments and analyses;
- Defines specific goals to guide prioritization, maturation, management, and use of assessments and analyses;
- Clarifies opportunities for collaboration and mutual support between assessments and analyses;
- Articulates opportunities to assist missions of other federal agency, including the Federal Emergency Management Agency (FEMA) and other agencies in risk assessments that support grant-allocation decisions; and
- Provides a plan to develop and use performance metrics for program management and reporting processes.

During implementation, this strategic plan will direct resource allocation for assessments. Additionally, regular progress reviews will be held to monitor the performance of the metrics detailed in the plan and to direct corrective actions as necessary. For more information on implementation of this strategic plan, see the section titled *Implementation*.

### III. Three-Year Strategic Plan

This 3-year strategic plan guides the selection and prioritization of assessments and also identifies the desired future state of maturity for assessments, the goals, and objectives that IP will pursue to get there. This plan was developed through a formal, repeatable strategic planning process that included a baseline analysis with a mission, organization, and tool review, as well as extensive stakeholder engagement and data-driven analysis. Table 1 depicts several process highlights.

| <b>Baseline Analysis</b>  |  |   |
|---|--|---|
| <b>Documentation type</b>   | <b>Quantity reviewed</b>   |   |
| <b>Government plans, guidance, and policy documents (e.g., NIPP, Presidential Policy Directive 21, IP sector-specific plans, and Government Coordinating Council and Sector Coordinating Council charters)</b>                      | <ul style="list-style-type: none"> <li>• 49 documents, plus information on DHS agency Web sites</li> </ul>   |   |
| <b>Congressional Budget Justification and Common Appropriations Schedule</b>  | <ul style="list-style-type: none"> <li>• 2 documents</li> </ul>  |   |
| <b>Congressional Research Service and Government Accountability Office reports</b>  | <ul style="list-style-type: none"> <li>• 5 documents</li> </ul>  |   |
| <b>Voluntary assessment documentation and summary reports (e.g., standard operating procedures, timelines, fact sheets, business practices, Industrial Control Systems Cyber Emergency Response Team [ICS-CERT] annual reports)</b> | <ul style="list-style-type: none"> <li>• 30 documents, plus 36 RRAP reports + assessment summary data on Infrastructure Protection Gateway (IP Gateway)</li> </ul> |   |
| <ul style="list-style-type: none"> <li>• <b>Background research on maturity models</b></li> </ul>   | <ul style="list-style-type: none"> <li>• 40 articles and reports</li> </ul>  |   |
| <b>Stakeholder Engagement</b>   |  |   |
| <b>Stakeholder category</b>   | <b>No. of interviewees</b>   | <b>No. of survey responses</b>  |
| <b>Key NPPD Stakeholders</b>  | <ul style="list-style-type: none"> <li>• 20 interviews</li> </ul>  |   |
| <b>Key IP Stakeholders</b>  | <ul style="list-style-type: none"> <li>• 20 interviews</li> </ul>  |   |
| <b>IP Community (e.g., sector-specific agencies (SSA), Emergency Support Function Leadership Group, Recovery Support Function Leadership Group, Mitigation Framework Leadership Group, Grant-making)</b>                            | <ul style="list-style-type: none"> <li>• 48 interviews</li> </ul>  | <ul style="list-style-type: none"> <li>• 44 survey responses</li> </ul> |

TABLE 1.–Summary of Baseline Analysis and Stakeholder Engagement Efforts

## Development of the Plan

This plan was developed through a three-phased process:

1. Understand the current, or “as-is,” state of assessments.
2. Identify the desired, or “to-be,” state of assessments.
3. Develop goals and objectives that will close the gap between the two states.

The “as-is” state provides baseline information about the current state of assessments. The “to-be” state identifies where leadership wants to take its assessments over the next 3 years. These two states were compared and goals and objectives were set to close the gaps. Metrics were developed to assess progress made against goals and objectives; these enable the demonstration of increasing maturity of assessments over time.

### “As-is” State

In order to understand the current (“as-is”) state of assessments, analysts first conducted a baseline analysis of IP’s mission, organization, and assessment tools by reviewing the following types of documents:

- Basic information on past facility assessments;
- RRAP reports;
- RRAP nomination and selection process information;
- ICS-CERT annual reports;
- Performance measures and reviews; and
- Assessment question sets.

Next, analysts reviewed sector-specific plans, Government Coordinating Council and Sector Coordinating Council charters, and other sources to catalog the “Stakeholder Landscape,” which includes those agencies involved in federally coordinated or sponsored critical infrastructure-related initiatives. From this robust list, analysts categorized stakeholders into bins that helped to streamline the type of information that each could contribute most realistically to this initiative, in order to gain as much value from the broadest number of stakeholders possible, without becoming a burden.

As part of the effort to understand the “as-is” state, analysts interviewed no fewer than 40 individuals from key NPPD stakeholder groups to fill gaps in the baseline analysis and to ensure a comprehensive and detailed understanding of current capabilities and plans.

Several noteworthy findings emerged from the “as-is” analysis:

- Assessment capabilities are particularly mature in the areas of IP’s ability to maintain data security, understanding user needs, and collecting assessment data. IP has set its highest maturity target on data security (sustainment and enhancement), intending to reach maturity fully in this area in 3 years.

- Priority stakeholders continue to include critical infrastructure owners/operators and the SLTT community, but many opportunities also exist to collaborate with interested federal agencies, such as FEMA; SSAs of lifeline sectors such as energy, water, or transportation; U.S. Department of Energy; U.S. Environmental Protection Agency; U.S. Department of Transportation; Transportation Security Administration; and U.S. Department of Agriculture.
- There is significant interest in—and potential to leverage much more value from—IP’s work through robust outreach to potential users, including providing information about completed and ongoing analyses, available data, and points of contacts.
- Critical infrastructure-related priorities identified by external agencies focus on lifeline functions, dependencies, and interdependencies.
- Usage of the IP Gateway<sup>2</sup> likely would increase if information (critical infrastructure data and reports) were easier to find within the system.

Appendix B, *The Current State: Findings and Stakeholder Needs*, provides a more extensive review of the as-is analysis, including findings from the baseline analysis and recommendations from stakeholders.

## “To-be” State

In order to begin to identify a “to-be” state, analysts expanded stakeholder engagement to include agencies external to NPPD. Nearly 100 additional stakeholders either were interviewed or responded to an inquiry to explain their critical infrastructure-related needs, priorities, and gaps. If they were familiar with voluntary assessments, they were asked about their experience—both positive and negative (i.e., indicating a need for improvement). If they were not familiar, they were asked about their critical infrastructure-related priorities and assessment needs. This, coupled with recommendations from the key stakeholders, provided granular information to inform a desired “to-be” state. The “to-be” state is defined both by future levels of desired maturity for assessments and by the goals and objectives to get there.

## Closing the Gap

In order to compare the “as-is” and “to-be” states in a useful and actionable way, a maturity model was created, which illustrates a high-level, 3-year plan in a succinct graphic and provides a structure to inform the development of goals and objectives that will close the gap between the two states. The rest of this plan provides details on these steps, as well as detailed outputs from the analyses described above.

---

<sup>2</sup> The IP Gateway serves as the single interface through which DHS partners can access a large range of integrated infrastructure protection tools and information to conduct comprehensive vulnerability assessments and risk analysis ([www.dhs.gov/ipgateway](http://www.dhs.gov/ipgateway)).

# Strategic Framework: The Voluntary Assessments Maturity Model

## The Approach to, and Benefits of, a Maturity Model

To provide a framework for the strategic planning process and the strategic plan, a Voluntary Assessments Maturity Model was developed. The maturity model provides a fixed benchmark, aligned with industry standards, against which operations can be assessed. It establishes a framework for understanding the current state of business processes, prioritizing and communicating the improvements that it wants to make, and developing an initial roadmap for how it will achieve its desired future state.

Government agencies and the private sector commonly use maturity models to assess processes and guide planning in areas such as software development, data management, and project management. By allowing organizations to compare their own processes to common practices industrywide, maturity models help them to identify areas for improvement and to track improvements over time. Benefits often include:

- Establishing a standard terminology for the high-level activities that an organization performs, so that the whole organization shares a common understanding of its operations;
- Providing a framework for envisioning the future state of an organization's operations, and for communicating what is needed to achieve it;
- Helping organizations to perform gap analyses between their current states and their desired futures, and leading them to begin planning for how to address the gaps; and
- Providing benchmarks against which organizations can measure progress internally, and providing a convenient mechanism for reporting progress externally.

All of these benefits are directly applicable to the Voluntary Assessments Maturity Model. The model is organized around five domains, which provide a standard framework for describing assessment processes. Within each domain, the model provides milestones based on common industry practices that can be used to illustrate by example how it should operate in the future. By evaluating current operations against the model's milestones, specific improvements can be identified, and these improvements can be prioritized and planned. Furthermore, by using the model to track progress over time, achievements easily are monitored internally and reported externally.

## Developing the Model

The assessment maturity model was developed initially by decomposing voluntary assessment operations into five top-level domains, and, on the basis of industry standards, further dividing them first into subelements, and then into topics under each subelement. (Appendix B provides a list of subelements and topics.) The five domains are as follows:

1. **Fitting Assessments to User Needs:** Ensuring that assessments data are useful to stakeholders and strategically identifying new opportunities to add value.
2. **Conducting Assessments:** Gathering, measuring, and recording assessment results.

3. **Managing Assessment Information:** Controlling, protecting, and delivering assessment data.
4. **Creating Analytic Products:** Enhancing the value of data through the creation and communication of analytical findings.
5. **Managing Data Quality:** Ensuring that assessments data are suitable for their intended purpose, as well as for future applications across planning and operations.

Analysts next defined four general stages of maturity that apply across domains. These stages, based largely on existing maturity models from other industries, include the following:

1. **Ad Hoc:** Activities tend to be reactive, inward-focused, and primarily carried out at the project or individual level.
2. **Emerging:** Activities occur in a structured, repeatable fashion, with higher forms of control (e.g., policies, governance bodies). There are indications of limited outward-looking activity and evidence of developing institutional capability.
3. **Established:** Activities occur under established structures, with evidence that these structures are followed consistently. Opportunities to enhance the value of current activities or increase efficiencies are explored and are anticipatory in nature. Considerations external to IP begin to influence decision-making.
4. **Optimized:** Established structures show evidence of proactive action and lifecycle and sustainment considerations. Focus shifts to strategic refinement and alignment of these structures with continuous improvement, feedback loops, and planning activities. Data are treated as integrated, enterprise-level assets.

Analysts developed a set of milestones that indicate a particular maturity level within each domain and subelement. If a milestone already has been realized, it contributes to the “as-is” state of assessment maturity. If IP aspires to realize that milestone over the next 3 years, it contributes to the “to-be” state of assessment maturity. These milestones provide an objective benchmark to assess current operations, and help to identify a desired state for future operations. Appendix B provides a full description of the maturity model subelements and milestones.

As process improvements are implemented, the maturity model can be used to monitor and report on progress. For example, annual reevaluations of the current status could alert managers to areas in which progress may be slower than desired, or they could help to demonstrate improved outcomes to staff. In addition, as the current state gets closer and closer to the desired future state over time, the maturity model can be included in reports to leadership such as Congress and DHS executives. Reassessing the desired future state as environmental challenges and opportunities evolve also can be part of a continuous improvement process. The maturity model serves as the strategic framework for this plan.

### Stages of Maturity

**Ad Hoc:** activities tend to be reactive and inward focused.

**Emerging:** activities occur in a structured, repeatable fashion; there are indications of limited outward-looking activity and evidence of developing institutional capability.

**Established:** activities occur under established structures, with evidence these structures are consistently followed; opportunities to enhance value are explored and are anticipatory; considerations external to IP begin to influence decision-making

**Optimized:** established structures show evidence of proactive action, and life-cycle and sustainment considerations; focus shifts to strategic refinement and alignment of these structures with continuous improvement, feedback loops, and planning activities; data is treated as an integrated, enterprise-level asset.

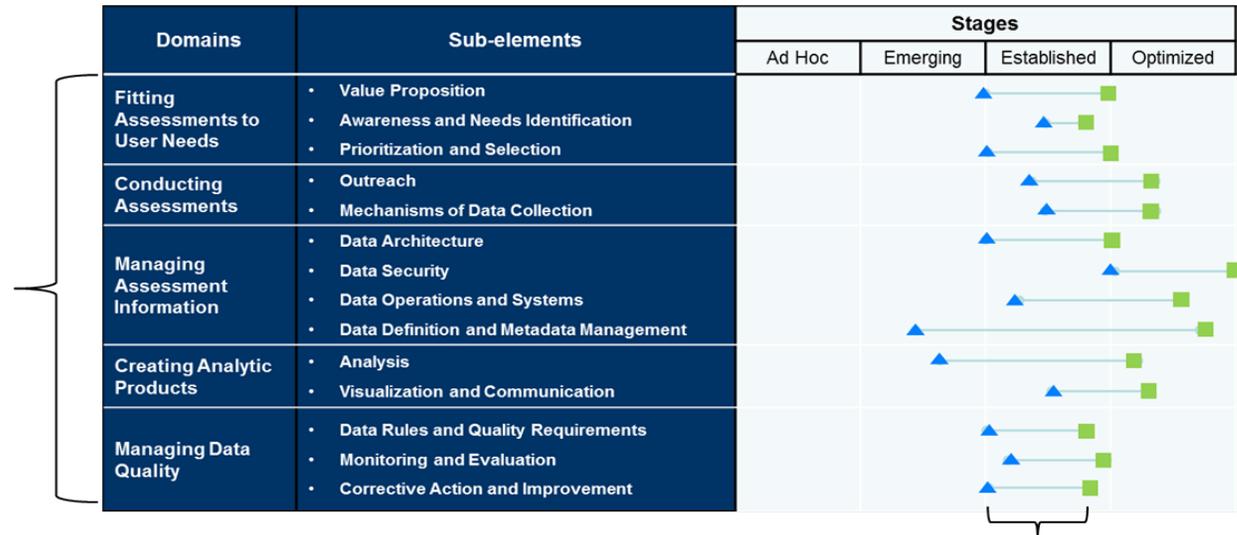
### Determining Placement of Symbols

Exact placement of triangles and squares is determined by the Maturity Model Placement Tool. A series of milestones based on industry standards and stakeholder inputs, refined to reflect assessment operations and needs, was developed. These milestones allow for tracking of progress through the four stages of maturity.

Milestones that are fully realized drive the placement of the triangles, or the “as-is” state; milestones that are scheduled for realization within the next three years, or the “to-be” state, drive the placement of the squares. See Appendix B for a listing of all milestones and their contributions to the maturity model.

## Voluntary Assessments Maturity Model

**Domains and Sub-elements**  
The domains and corresponding sub-elements are based on a decomposition of all operations related to voluntary assessments. They, along with their measures of current and desired maturity, constitute a framework to drive IP's strategic planning efforts.



The Strategy's goals and objectives are designed to help close the gap between the as-is and the desired to-be states.

- ▲ Indicates the current, “as-is” state for each sub-element, established through baseline analysis and stakeholder engagement, validated by NPPD leadership during the first of three stakeholder workshops comprising this strategic planning process
- Indicates the desired “to-be” state three years from now for each sub-element, suggested by stakeholder engagement, validated by NPPD leadership during the second of three stakeholder workshops comprising this strategic planning process

FIGURE 1.–Voluntary Assessments Maturity Model

## IV. The Future State: Goals, Objectives, and Metrics

IP envisions that every voluntary assessment and analysis will improve risk management locally and enhance the Federal Government's ability to manage infrastructure risk nationally. As discussed previously, a series of goals and objectives structured around the maturity model has been developed, which will guide efforts to sustain and mature the assessment enterprise over the next 3 years. The goals and objectives define priority areas of focus over the next 3 years and will be reviewed and updated annually, as necessary. They also are informed by the findings described earlier in this report, and the findings will be addressed even more specifically in the upcoming implementation plan. Some of the objectives likely will carry over from year to year, while others may be removed or updated on the basis of progress and actual needs. Table 2 provides a summary of the goals and objectives organized by the five maturity model domains.

The remainder of this section provides a more in-depth look at the goals, objectives, and metrics. As described earlier, goals and objectives are organized around each domain of the maturity model. In most cases, there is one goal per subelement of the maturity model, so that attention remains focused on progressing maturity of programs according to agreed-upon desired end-states (3 years from now). There are two exceptions when goals apply to more than one subelement. Objectives are the measurable activities that must be performed to realize the goals; these are still high-level activities and should be decomposed further for implementation. Finally, each domain includes the quantitative metrics that will be used to assess progress toward achieving the goals and objectives.

TABLE 2.–Summary Three-Year Strategic Plan for Objectives

| Domain  | Goals  | Objectives  |
|---|--|---|
| <b>Align Assessments to User Needs</b>              | 1.1: Ensure that stakeholders drive the voluntary assessments’ value propositions and subsequently, assessment-related work. | 1.1.1. Establish a process to revisit and update value propositions based on stakeholder input, both internal and external to IP.<br>1.1.2. Establish a process to consider revisions or overhauls to assessments and products (or creation of new products) based on value propositions (e.g., supporting the THIRA).<br>1.1.3. Develop materials that effectively communicate value propositions.                                 |
|   | 1.2: Continuously expand relationships with entities identified in the stakeholder landscape.                                | 1.2.1. Create and maintain an outreach plan that identifies high-priority stakeholder groups and addresses customized outreach materials.<br>1.2.2. Ensure that all IP staff engaged in outreach activities have requisite knowledge of assessments.<br>1.2.3. Track interactions with users and customers through a defined process and tool.<br>1.2.4. Establish a mechanism to collect user and customer needs and requirements. |
|   | 1.3: Maintain a strategy for the selection and prioritization of assessment-related decisions.                               | 1.3.1. Clearly delineate decision-making roles and responsibilities of headquarters, the regions, and assessors.<br>1.3.2. Establish a prioritization model for the assessment of infrastructure to realize value propositions.   |
| <b>Mature Conduct of Assessments</b>                | 2.1: Expand participation of users and customers in assessments.   | 2.1.1. Identify target levels of participation in assessments and incentivize that participation.<br>2.1.2. Review and refine existing processes for collecting user and customer feedback and for recommending specific enhancements to assessment tools.  |
|   | 2.2: Ensure appropriate processes and resources to conduct assessments effectively.  | 2.2.1. Keep training current to ensure the efficient transfer of the knowledge, skills, and abilities necessary to conduct assessments.<br>2.2.2. Align assessment efforts to resources.<br>2.2.3. Streamline information technology processes that enable assessors to conduct assessments optimally.  |
| <b>Improve Management of Assessment Information</b> | 3.1: Expand user access to assessment data.  | 3.1.1. Identify desired use cases, data formats, and mechanisms for data access as part of user outreach efforts.<br>3.1.2. Identify needed changes to existing data architecture to accommodate assessment value propositions.   |
|   | 3.2: Maintain an appropriate level of data security while encouraging data sharing.  | 3.2.1. Develop a risk management plan that addresses integration of data sets and user access to data.<br>3.2.2. Manage risk by sustaining and updating training and data security monitoring programs.<br>3.2.3. Communicate data security policies and practices to stakeholders to improve awareness of data security and permissions.   |
|   | 3.3: Improve support that assists users and customers in using assessment data effectively and correctly.                    | 3.3.1. Collect feedback from users and customers to identify and prioritize data use challenges.<br>3.3.2. Address data use challenges through training, technical assistance, and data management.<br>3.3.3. Integrate assessment datasets, such as IP, OCIA, and Office of Cybersecurity and Communications datasets, through one or several common identifier(s).  |
| <b>Create Actionable Analytic Products</b>          | 4.1: Continuously enhance analytic quality and capabilities.   | 4.1.1. Establish a transparent, formal process for the identification, assignment, scoping, and execution of analyses.<br>4.1.2. Build out capability to perform rapid analyses.<br>4.1.3. Explore innovative analytic techniques that might increase the value provided by assessment data.  |
|   | 4.2: Provide actionable analytic products to all users and customers.  | 4.2.1. Develop capabilities to produce increasingly sophisticated analytics and visualizations to facilitate decision-making.<br>4.2.2. Ensure that users and customers understand how analytic results are derived.<br>4.2.3. Incorporate user and customer feedback to improve analytic products continuously.  |

| Domain   | Goals   | Objectives  |
|--|---|---|
| <b>Strengthen<br/>Management<br/>of Data<br/>Quality</b> | 5.1: Establish data quality criteria for all assessments. | 5.1.1. Establish data rules and quality requirements on the basis of the criticality of data elements, and link them to data monitoring efforts.<br>5.1.2. Elicit quality requirements for data requests from all users and customers.  |
|  | 5.2: Track and address data quality issues.               | 5.2.1. Establish a method to log information from data quality monitoring efforts.<br>5.2.2. Establish processes to address data quality issues identified through monitoring activities or feedback from users.<br>5.2.3. Analyze data quality issues to identify the root causes of problems. |

## V. Implementation

The following section provides an initial outlook on the way ahead for implementation of this strategic plan, which includes a look at governance, execution, prioritization and selection of assessments, and challenges and opportunities.

### Governance

The performance of IP assessments against the multiyear priorities and objectives outlined in this plan will be integrated into existing and future strategic planning, budget, and quarterly program review performance management activities.

### Execution

The goals and objectives outlined in the above plan are ambitious but attainable. To ensure that the goals in this strategic plan are accomplished successfully, IP and OCIA will develop an implementation plan to support the strategic plan. The implementation plan will outline the roles and responsibilities associated with each goal/objective, including goal/objective ownership; objective dependencies and assumptions; activities to undertake each fiscal year in support of the objective; and the detailed milestones, owners, and timelines for FY 2018 to FY 2020 activities.

Tables 3 and 4 provide a review of interdependencies and stakeholder priorities among objectives, to provide some guidance for the development of a specific implementation plan. Each activity represents an objective. A checkmark indicates that an activity is scheduled preliminarily for execution to begin either in the first, second, or third phase of implementation. This is based primarily on leadership priorities and, in some cases, on the need for certain activities to begin prior to others. Because there are many objectives in this strategic plan pertaining to stakeholder engagement, activities required to accomplish the body of outreach-related objectives are grouped and prioritized rather than listed verbatim as they appear in the plan.

TABLE 3.–Activity by Domain

| Activity (Objective) by Domain   | 1 <sup>st</sup> | 2 <sup>nd</sup> | 3 <sup>rd</sup> |
|--|-----------------|-----------------|-----------------|
| <b>Fitting Assessments to User Needs</b>   |                 |                 |                 |
| • Initiate and implement outreach and a requirements collection program*   | ✓               |                 |                 |
| • Establish an infrastructure prioritization model (1.3.2)   | ✓               |                 |                 |
| • Clearly delineate decision-making roles across HQ, the regions, and assessors (1.3.1)                              |                 | ✓               |                 |
| <b>Conducting Assessments</b>  |                 |                 |                 |
| • Review and update training for assessors (2.2.1)   | ✓               |                 |                 |
| • Train NPPD staff to support assessments (2.2.2)  |                 | ✓               |                 |
| • Identify target levels of participation in assessments and incentivize participation (2.1.1)                       |                 |                 | ✓               |
| <b>Managing Assessment Information</b>   |                 |                 |                 |
| • Develop a risk management plan that addresses integration of data sets and user access to data (3.2.1)             |                 | ✓               |                 |
| • Integrate assessment datasets (3.3.3)  |                 | ✓               |                 |
| • Manage risk by sustaining and updating training and data security monitoring programs (3.2.2)                      |                 |                 | ✓               |
| <b>Creating Analytic Products</b>  |                 |                 |                 |
| • Establish a transparent, formal process for identification, assignment, scoping, and execution of analyses (4.1.1) | ✓               |                 |                 |
| • Ensure users and customers understand how analytic results are derived (4.2.2)                                     | ✓               |                 |                 |
| • Build-out capability embedded in IP to perform rapid analyses (4.1.2)  | ✓               |                 |                 |
| • Produce increasingly sophisticated analytics and visualizations (4.2.1)  |                 | ✓               |                 |
| • Explore innovative analytic techniques (4.1.3)   |                 |                 | ✓               |
| <b>Managing Data Quality</b>   |                 |                 |                 |
| • Establish data rules and quality requirements based on the criticality of data elements (5.1.1)                    | ✓               |                 |                 |
| • Establish a process to log and address data quality issues (5.2.1)   |                 | ✓               |                 |
| • Analyze data quality issues to identify root causes (5.2.3)  |                 |                 | ✓               |

\*A significant number of objectives relate to stakeholder engagement and requirements collection, and are built out into their own table below.

TABLE 4.–Stakeholder Engagement and Requirements Collection-related Activities

| Stakeholder Engagement- and Requirements Collection-related Activities (Objectives)   | 1 <sup>st</sup> | 2 <sup>nd</sup> | 3 <sup>rd</sup> |
|---|-----------------|-----------------|-----------------|
| <p><b>Create an Outreach and Requirements Collection Plan</b> that will:</p> <ul style="list-style-type: none"> <li>• Identify high priority stakeholder groups (1.2.1)</li> <li>• Re-visit and update value propositions (1.1.1)</li> <li>• Collect feedback on assessment tools (2.1.2)</li> <li>• Communicate data security policies (3.2.3)</li> <li>• Identify desired use cases, data formats, and mechanisms for data access (3.1.1)</li> <li>• Identify data use challenges (3.3.1)</li> <li>• Elicit quality requirements for data (5.1.2)</li> <li>• Collect feedback on analytic products (4.2.3)</li> </ul> | ✓               |                 |                 |
| <b>Implement the Outreach Plan</b>  |                 | ✓               |                 |
| <b>Track interactions with users and customers through a defined process and tool (1.2.2)</b>   |                 | ✓               |                 |
| <p><b>Use feedback collected through Outreach Plan</b> to:</p> <ul style="list-style-type: none"> <li>• Log and prioritize needs and requirements (1.2.3)</li> <li>• Update value propositions (1.1.1)</li> <li>• Revise and/or overhaul existing assessments (1.1.2)</li> <li>• Revise and/or overhaul existing analytic products (1.1.2)</li> <li>• Create new assessments or products (1.1.2)</li> <li>• Modify existing data architecture (3.1.2)</li> <li>• Address data use challenges (3.3.2)</li> </ul>   |                 |                 | ✓               |

## Prioritizing Voluntary Assessments

A major priority and a key driver behind the development of this strategic plan is the need to define a clear prioritization strategy for the selection and execution of voluntary assessments. The strategic planning process conducted to develop this document included a stakeholder engagement program, which revealed broad interest and buy-in to this intent. Goal 1.3 addresses this directly: *Maintain a strategy for the selection and prioritization of assessment-related decisions*, and the upcoming implementation plan will outline the specific steps needed to put a long-term, sustainable prioritization strategy into place.

To accomplish this, IP and OCIA will conduct an annual Assessment Prioritization Session. The purpose of this annual session is twofold. First, it will establish that year’s criteria, on the basis of current value propositions, which will guide assessment-related decision-making. Second, it will lay out a plan to prioritize stakeholder needs and requests, which align with IP assessment and OCIA analysis value propositions and balance limited resources across assessment types, such as RRAPs, Infrastructure Survey Tools, and Rapid Survey Tools. During the session, stakeholders will examine the implications of the value propositions on existing assessments and will consider additional factors such as progress toward completing representative samples of assessments per sector, emerging threats, and stakeholder priorities to refine assessment criteria

and distribution further. The session will include meaningful discussions about emerging threats and competing priorities before making final assessment decisions. At the conclusion of the first year's Assessment Prioritization Session, IP and OCIA will codify the prioritization process and will review specific assessments to ensure that they are producing data that are aligned to the value propositions.

Five key questions emerged that encapsulate the most commonly expressed stakeholder needs:

| 5 Key Questions to Assist in Assessment Prioritization   |
|--|
| <ul style="list-style-type: none"><li>• Does this effort address <b>prioritized critical infrastructure and/or a lifeline function</b> in some way?</li><li>• Does this effort further our understanding of threat, vulnerabilities, or consequences related to <b>cybersecurity</b>?</li><li>• Does this effort address <b>dependencies, interdependencies, and/or cascading consequences</b> across sites, networks, sectors, or even jurisdictions?</li><li>• Does this effort help us to see any of the above accurately on a <b>map</b>?</li><li>• Does this effort directly result in the <b>identification of trends</b> across a sector, a region, or the country?</li></ul> |

If a potential assessment can address at least one of these questions, it is eligible for prioritization. If it addresses more than one of these questions, its priority increases. Part of the long-term, sustainable assessment prioritization process will be to keep these questions updated so that at any time, IP and OCIA can cite them to explain how assessments are prioritized.

## Challenges and Opportunities

Over the next 3 years, IP assessments will face a number of challenges and risks that potentially could impede progress toward the strategic goals and objectives articulated in this document. IP also can take advantage of the opportunities presented by the institutional changes that will occur over the next 3 years.

### Challenges

The voluntary nature of IP assessments presents an enduring challenge that must be incorporated into the strategic and operational planning that guides the future of the assessments. This highlights the importance of clearly articulated value propositions that can be used to encourage participation in the program. It is incumbent on IP to be able to define clearly and consistently how private-sector partners benefit from conducting assessments, how they benefit from broader participation in the assessment program, and what incentives exist to drive further participation on individual and systemic levels. Assessments also need to demonstrate that they can be responsive to and mitigate any potential concerns that regularly arise when discussing voluntary participation with the program.

A second major challenge for IP assessments is that the threat environment is rapidly changing, which means that assessments must be sufficiently flexible and responsive. Although assessments are, by nature, decentralized, sufficient information and threat-sharing mechanisms must be maintained to ensure that shifts in the threat environment are captured and analyzed, and that their impacts shape assessment outputs.

Another enduring challenge for assessments will be resourcing. Because the program is completely voluntary and nonreimbursable, as assessments begin to integrate new tools, capabilities, and goals over the next 3 years, one key step will be ensuring that available resources are managed through prioritization and objective-setting discussions that address both program implementation and program improvement.

## **Opportunities**

The biggest opportunity that exists for IP to increase the profile and effectiveness of its assessments is the ongoing work toward enhanced regionalization. That work is aimed at shifting the center of gravity for IP operations from headquarters to the field, and it encompasses an array of personnel, functions, and operational shifts. The goal of regionalization is to improve the delivery of services to stakeholders and to enhance support for existing field forces that include DHS PSAs. The regionalization effort will provide an opportunity for IP to implement any desired changes for its assessments, because it can encourage a discussion about what capabilities are needed in the field to organize, conduct, and analyze assessments more effectively.

Another opportunity for assessments is to work with internal stakeholders to identify ongoing projects within NPPD that could be used to help promote the use of assessments and related data. From priority setting to annual reporting, NPPD works in a number of areas that could benefit if IP had access to the direct stakeholder inputs gathered through voluntary assessment activities. Moreover, the suite of assessments also can identify NPPD programs that IP could leverage to promote participation in the suite of assessments by broadening its outreach base, as well as by building support for participation both within all levels of governments and with private-sector stakeholders by demonstrating the impact that participation can have. Each region has a Sector Outreach Coordinator who works directly with owner operators and conducts outreach but does not do assessments. These two elements work in concert at the regional level to determine priorities.

Annual assessment priorities are dynamic—and often must respond to shifts in threats and hazards, or exigent challenges resulting from real-world events. Although the annual prioritization process provides the framework for activity, PSAs and Regional Directors maintain flexibility in selection and conduct of assessments.

## VI. Conclusion

This strategic planning process has established a clear path forward for NPPD voluntary assessments. By comprehensively reviewing the core components of the assessment enterprise and by engaging customers and stakeholders to understand their priorities and needs better, strengths and challenges of the assessments have been identified. By executing the goals and objectives outlined in this plan over the next 3 years, IP assessments and OCIA analyses will result in significantly more value for critical infrastructure owners/operators and federal partners alike, thus strengthening IP's ability to improve the security and resilience of the Nation's critical infrastructure.

The strategic plan describes a new annual prioritization process, but also lays out initial priorities for voluntary assessments. The annual process will ensure a connection between regional priorities—based on direct relationships with partners—and national priorities based on sector engagement efforts and changes in the risk environment nationally.

# Appendices

## Appendix A: Suite of IP Voluntary Assessments, Analyses, and Programs

The Department of Homeland Security (DHS) conducts a broad range of assessments for critical infrastructure. This strategic plan applies to the existing suite of the Office of Infrastructure Protection’s (IP) voluntary assessments, analyses, and programs. Table 5 characterizes and identifies the eight assessment tools and programs that currently make up IP’s voluntary suite of assessments.

This strategic plan is focused on IP voluntary assessments only and does not pertain to regulatory inspection programs or federal facility security designations.

TABLE 5.–Suite of IP Voluntary Assessments, Analyses, and Programs

| Focus  | Assessment Tool / Program              | Description  | Product / Output   | Responsible Organization   |
|--|--|--|--|--|
| <b>Facility Specific: Physical</b>                 | Infrastructure Survey Tool (IST)       | Collects structured information on facilities’ physical security, security-management procedures, security logistics, preparedness, dependencies, and risk components (threats, vulnerabilities, and consequences)   | Assists facilities in assessing security and resilience posture with respect to peer facilities through the generation of interactive dashboards that display resilience and protective indices  | DHS/National Protection and Programs Directorate (NPPD)/IP/ Protective Security Coordination Division (PSCD) |
|  | Site Assistance Visit                  | An in-depth assessment conducted by a team of DHS assessors, often for large and complex sites or for those hosting special events (e.g., a university campus)   | Assessors verbally communicate security, resilience, and mitigation strategies to critical infrastructure owners and operators, followed by a written summary report   | DHS/NPPD/IP/ PSCD  |
| <b>Facility Specific: Physical/ Cyber</b>          | Rapid Survey Tool (RST)                | Collects structured information on facilities’ physical security, dependencies, preparedness, cyber policies, risk components, security logistics, and security management (The RST is shorter than the IST and includes a cyber component.)   | Assists facilities in assessing security and resilience posture with respect to peer facilities through the generation of interactive dashboards that display resilience and protective indices  | DHS/NPPD/IP/ PSCD  |
| <b>Facility Specific: Dependencies</b>             | Dependency Survey Tool                 | Collects structured information on facilities’ critical dependencies, including lifeline functions like water and electricity  | Assists facilities in assessing the resilience of critical services provided by external sources   | DHS/NPPD/IP/ PSCD  |
| <b>Regional: Physical, Cyber, and Dependencies</b> | Regional Resiliency Assessment Program | Long-term, large-scale projects that fall into three broad categories:<br>1) characterization projects, which seek to set a baseline understanding of infrastructure function, structure, operations, and vulnerabilities for a given region (e.g., by sector, system, or network); 2) dependency analyses, which examine the nature of dependencies and interdependencies between infrastructure systems and sectors across a region; and 3) hazards analyses, which rely on characterization and dependency analyses to assess the direct and cascading impacts of given hazards to infrastructure | Provide more consistent understanding of infrastructure and related issues across the range of partners involved in regional critical infrastructure protection activities, and drive concerted action to improve infrastructure security and resilience | DHS/NPPD/IP/ PSCD  |

## Appendix B: The Current State: Findings and Stakeholder Needs

This section provides findings from all of the analysis conducted, organized by maturity model domain. Each domain includes:

1. A brief description of the domain;
2. Findings that emerged from the baseline analysis, which included a mission, organization, and tool review developed through literature and interviews; and
3. A table that outlines specific recommendations from the stakeholder engagement program, including key stakeholders, as well as users and potential users from key government agencies.

### Domain 1: Fitting Assessments to User Needs

This domain includes all activities associated with clarifying how assessments data can and should be employed to meet user needs, as well as strategically identifying new opportunities to add value. In achieving these activities, IP must set, understand, and promulgate its value propositions clearly. To meet user needs, IP also must identify specific requirements from a wide group of stakeholders. Finally, IP must develop and commit to a prioritization and selection method that drives assessment activities.

**Finding: Primary stakeholders are critical infrastructure owners/operators, because these partners enable IP to collect infrastructure security and resilience information and, thereby, realize all value propositions of IP assessments and OCIA analyses.**

Accordingly, IP should continue to engage critical infrastructure owners/operators and prioritize additional engagement with interested external federal partners whose critical infrastructure needs align with the value propositions and are mentioned in key policy. These proposed approaches to stakeholder prioritization are depicted in Table 6 and Figure 2 below.

TABLE 6.—Stakeholder Groups in Priority Order

| Stakeholder Groups in Priority Order  |
|---|
| 1. Current customers (critical infrastructure owners/operators)                       |
| 2. Potential customers (critical infrastructure owners/operators)                     |
| 3. State, local, tribal, and territorial (SLTT) agencies                              |
| 4. Prioritized federal partners (current or potential users)                          |
| 5. All other potential users (e.g., other federal partners, stakeholder associations) |

**Finding: Assessments are designed to maximize owner/operator participation.** IP and Office of Cybersecurity and Communications (CS&C) personnel that administer the eight assessments are aware that critical infrastructure owners/operators are the primary customer, and assessments are designed with their preferences and needs in mind. All but one assessment—the Regional Resiliency Assessment Program (RRAP)—can be accomplished in less than a day. This is critical to achieving critical infrastructure resilience and contributes to relationship-building activities with owners/operators.

**Finding: Assessments need to evolve with the emerging needs of stakeholders.** Although assessors note that critical infrastructure owners/operators are interested in interdependencies with other sectors that affect continuity of their operations, most assessments focus specifically on either physical or cyber security as they relate to a single facility. New assessment tools in development are beginning to focus on interdependencies. Additionally, the RST, which does include both physical and cyber assessments, typically is not used to fill this gap and may benefit from updates. Meanwhile, cyber and physical security assessments (and their associated tools) remain largely separate.

During the course of this strategic planning process, nearly 250 needs and requirements were identified from stakeholder engagement with federal partners alone. This number easily can grow significantly as a more widespread program of stakeholder engagement is pursued. Implementation of this strategy must include comprehensive outreach to current and potential federal partners, as well as to SLTT and private-sector customers and potential customers. Currently identified needs and requirements address both the assessments, themselves, and the process that surrounds the assessments; particular focus areas include: lifeline functions, cybersecurity, dependencies and interdependencies, map-based data, and trend analysis. Stakeholders explained that they would start (or expand) use of IP's assessment data if more of their needs were met. Almost all stakeholders engaged explained that they could see value or potential value in assessment work and hoped to leverage it to support their own missions and activities.

**Finding: There are many opportunities to modify assessment tools and analyses to leverage more value across the entire homeland security community.** This is true both during planning while in the steady state, and during response to real-world events and incidents. Partners such as the Federal Emergency Management Agency (FEMA) are interested in risk, hazard, and mitigation information, and response agencies are interested in critical infrastructure-related information that supports crisis decision-making and planning. Almost all assessments are focused at the single-facility level, and data is difficult to aggregate, limiting its utility to stakeholders interested in examining nationwide priorities.

However, the requirements of federal partners need to be balanced carefully against the needs of IP's top-priority stakeholder group: the owners and operators of critical infrastructure. IP's ability to meet federal needs would be lessened if continued attention and effort were not directed at maintaining an appropriate level of assessment support to owners/operators, because it is through this relationship that IP is able to assist in meeting the needs of other federal agencies.

FEMA, the U.S. Department of Energy, U.S. Environmental Protection Agency, U.S. Department of Transportation, Transportation Security Administration, and U.S. Department of Agriculture stand out as particularly good candidates for additional collaboration on the basis of these partners' mentions in key policy and outcomes from engagement efforts during the development of this strategic plan (i.e., expressed needs and requirements, interest in collaboration with IP). Figure 2 below provides an overview of criteria for assessing how best to support federal partners through IP assessments.

FIGURE 2.—Priority Federal Partners based on Key Policy and Outreach and Engagement Outcomes<sup>3</sup>

| Federal Partner                             | PRIORITIZATION CRITERIA |   |   |  |                                |
|---|-------------------------|---|---|--|--------------------------------|
|   | Identified in PPD-21    | Identified in DHS Appropriations Bill, 2016 | Identified as SSA for lifeline function in NIPP | Outcomes from initial outreach and engagement                                  |                                |
|   |                         |   |   | Needs / requirements align to 6 IP value propositions (6 check marks possible) | High interest in collaboration |
| Federal Emergency Management Agency         |                         | ✓   |   | ✓✓✓✓✓✓   | ✓                              |
| U.S. Dept. of Energy                        | ✓                       |   | ✓   | ✓✓   | ✓                              |
| U.S. Dept. of Agriculture                   | ✓                       |   |   | ✓✓✓  | ✓                              |
| Environmental Protection Agency             | ✓                       |   | ✓   | ✓  | ✓                              |
| U.S. Dept. of Transportation                | ✓                       |   | ✓   | ✓  | ✓                              |
| Transportation Security Administration      | ✓                       |   | ✓   | ✓  | ✓                              |
| U.S. Dept. of Defense                       | ✓                       |   |   | ✓✓   | ✓                              |
| U.S. Dept. of Health and Human Services     | ✓                       |   |   | ✓✓   | ✓                              |
| U.S. Dept. of Interior                      | ✓                       |   |   | ✓✓   | ✓                              |
| National Security Council                   | ✓                       |   |   | ✓✓   | ✓                              |
| U.S. Dept. of Treasury                      | ✓                       |   |   | ✓✓   | ✓                              |
| U.S. Dept. of Housing and Urban Development |                         |   |   | ✓  | ✓                              |

**Finding: There needs to be a defensible, repeatable process for prioritizing assessments.** Some general guidance is provided to NPPD Protective Security Advisors (PSA) in the IST standard operating procedures document, and there is a newly updated and well-received scoring rubric for RRAPs. However, there is no overarching process for determining the overall balance of the assessment portfolio. Prioritization and selection are often functions of funding, staffing limitations, and a desire to reach external assessment objectives (e.g., number of ISTs conducted), rather than as part of a cohesive strategy.

**Finding: Assessors would benefit from greater clarity on the full range of NPPD assessments available, to advise potential users and customers better on the best path forward.** Although IP and CS&C staff/assessors have clear understandings of their own assessments, they may not always be consistently aware of the full range of available assessments being conducted, and they may not have a clear understanding of the scope of each assessment. More robust internal information-sharing may help assessors provide additional guidance to their customers.

**Stakeholder Needs:** Table 7 outlines recommendations from the stakeholder engagement program related to Domain 1. Appendix D offers additional examples of stakeholder needs and requests organized by key topic areas of interest, such as analysis/report topic, RRAPs, and outreach topics.

<sup>3</sup> Additional federal partners also have been approached to discuss how IP can serve them better through its assessments. These partners include FEMA Grant Programs Directorate, National Institute of Standards and Technology, National Oceanic and Atmospheric Administration, U.S. Department of Education, U.S. General Services Administration, and Office of Management and Budget.

TABLE 7. –Recommendations for Fitting Assessments to User Needs

| <b>Domain 1: Fitting Assessments to User Needs</b> |  |
|--|--|
| <b>Stakeholder Group</b>                           | <b>Recommendations</b>   |
| <b>Key IP and NPPD Stakeholders</b>                | <ul style="list-style-type: none"> <li>• IP and OCIA should work more with FEMA because there are many opportunities for collaboration, including Threat Hazard Identification and Risk Assessments (THIRA) inputs, grant reviews, and plan reviews.</li> <li>• NPPD needs a tool to track all stakeholder activity and interactions with stakeholders across all divisions, such as a Customer Relations Management Tool.</li> <li>• DHS IP needs to become more directly involved in state and local relationships to understand customer needs more clearly; also, more focus is needed on private-sector owners and boards, not just operators.</li> <li>• Protected Critical Infrastructure Information (PCII) must be understood better by everyone, including IP staff, potential users, and even current customers, to encourage more participation in voluntary assessments.</li> <li>• Assessors would benefit from a deeper understanding of a variety of NPPD products—such as OCIA analytic products about expected impacts and cascading effects of an emergency, maps and geospatial services, and existing processes that push notifications of analytic products out to interested parties—to support users further and to collect analytic requirements more effectively.</li> <li>• IP should rethink its approach to the prioritization of assessments, including the following:             <ul style="list-style-type: none"> <li>○ Assessment decisions based on prioritized infrastructure lists.</li> <li>○ IST quotas can dissuade the pursuit of RRAP ideas because of too much burden on a single assessor.</li> <li>○ Statistical sampling to inform these decisions might be an effective idea worth pursuing.</li> <li>○ Regional directors are of high interest to stakeholders; stakeholders indicated that having regional directors would support improvements to the way assessments are prioritized and performed.</li> </ul> </li> </ul> |
| <b>Federal Agencies External to NPPD</b>           | <p><b>Outreach</b></p> <ul style="list-style-type: none"> <li>• Information about current products available—assessment data and analyses that have been completed—should be made available to current and potential users.</li> <li>• Synopses of findings from analyses, available for distribution, would be useful.</li> <li>• Information about analyses underway would be of interest to other federal agencies, including how they can get involved.</li> <li>• Points of contact for IP staff leading different initiatives and assessments so users can contact them for further information.</li> </ul> <p><b>Data</b></p> <ul style="list-style-type: none"> <li>• Federal agencies are interested in more training on Infrastructure Protection Gateway (IP Gateway), including live training.</li> <li>• Improved search features to locate specific data in IP Gateway (e.g., a specific site assessment, answers to a specific question) was requested repeatedly.</li> <li>• Data related to interdependencies was requested repeatedly.</li> <li>• Data related to cyber was requested repeatedly.</li> </ul> <p><b>Reports/Analyses</b></p> <ul style="list-style-type: none"> <li>• Reports and analyses that address dependencies and interdependencies are of high interest to stakeholders; they were requested repeatedly.</li> </ul>   |

| Domain 1: Fitting Assessments to User Needs |   |
|---|---|
|   | <ul style="list-style-type: none"> <li>• Reports and analyses that address lifeline functions (e.g., power grid, water sector, cyber impacts on lifelines) were specified as specific topics of interest.</li> </ul> <p><b>Other</b></p> <ul style="list-style-type: none"> <li>• Stakeholders indicated an interest in:               <ul style="list-style-type: none"> <li>○ Services—critical infrastructure information during emergencies</li> <li>○ Services—support for plan review and inputs, such as THIRA, Regional Catastrophic Plans, and Grant Applications</li> <li>○ Map Products—Locations of vulnerable critical infrastructure by threat type or any infrastructure-related information</li> <li>○ Map Products—Maps of cascading consequences</li> <li>○ Process—Pushing pre-identified information to interested parties (rather than making them find it on their own) would be beneficial.</li> </ul> </li> </ul> |

**Domain 2: Conducting Assessments**

This domain includes activities associated with gathering, measuring, and recording information of interest. In achieving these activities, stakeholder outreach must occur (focusing on current and potential users and customers), and efficient, repeatable, and effective mechanisms of data collection must be developed that place a minimal burden on those being assessed.

**Finding: The process for conducting assessments varies, depending on functional and geographic scope, method (facilitated or self-guided), and duration.**

- **Functional scope:** IST is the only assessment focused solely on physical security. Three CS&C assessments are focused solely on cybersecurity: the Cyber Infrastructure Survey Tool (C-IST), the Cyber Resiliency Review (CRR), and the Cyber Security Evaluation Tool (CSET). The RST is focused on both physical security and cybersecurity, and the RRAP has an unrestricted focus.
- **Geographic scope:** None of the assessments examined has a jurisdictional focus. IST, RST, and CSET are focused on individual facilities; CRR and C-IST focus on critical services and may or may not have geographic scope; and RRAP is regional.
- **Assessment method:** C-IST and RRAP have to be facilitated by a PSA or Cyber Security Advisor (CSA). The other assessments can be facilitated by a PSA or CSA, but also can be completed through a self-guided process.
- **Duration:** C-IST and RST can be completed in approximately 4 or fewer hours; CRR, CSET, and IST require between 4 and 8 hours to complete; CSET takes more than a day; and RRAP, which is a multi-faceted assessment process, can take more than a year to complete.

**Finding: The distribution of ISTs and site assistance visits (SAV) over sectors and location varies widely, and often is based on willingness to be assessed rather than on projected consequence or threat.** Some sectors are well represented in completed ISTs and SAVs. Six sectors—Commercial Facilities, Government Facilities, Energy, Healthcare and Public Health, Transportation, and Water and Wastewater Systems—each had more than a combined total of 500 PSA-led ISTs/SAVs completed from FY 2008 through FY 2016 (see Figure 3). Others are underrepresented. For example, PSAs have completed fewer than a combined total of 100

ISTs/SAVs each for six sectors: Chemical and Hazardous Materials Industry; Defense Industrial Base; Information Technology; Critical Manufacturing; Nuclear Reactors, Materials, and Waste; and Postal and Shipping (now part of Transportation). (There are good reasons for this: chemical facilities have vulnerability assessments performed under the Chemical Facilities Anti-Terrorism Standards program, nuclear facilities by the Nuclear Regulatory Commission, the Defense Industrial Base by the Defense Security Service, etc.) Similarly, although all states and territories had PSA-led ISTs completed from FY 2010 through FY 2016, the numbers vary greatly between them, and a handful of states have seen disproportionately more ISTs (see Figure 4).

FIGURE 3.—Aggregated PSA-led ISTs and SAVs by sector, FY 2008–FY 2016

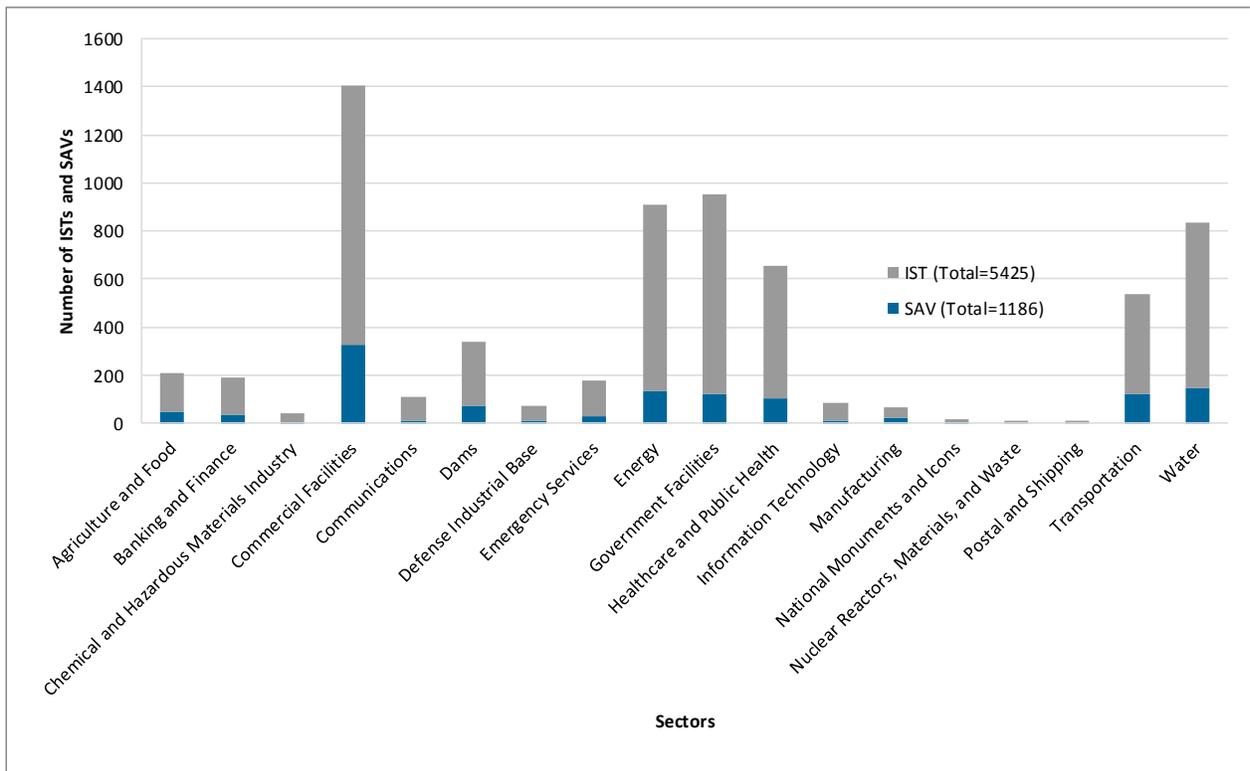
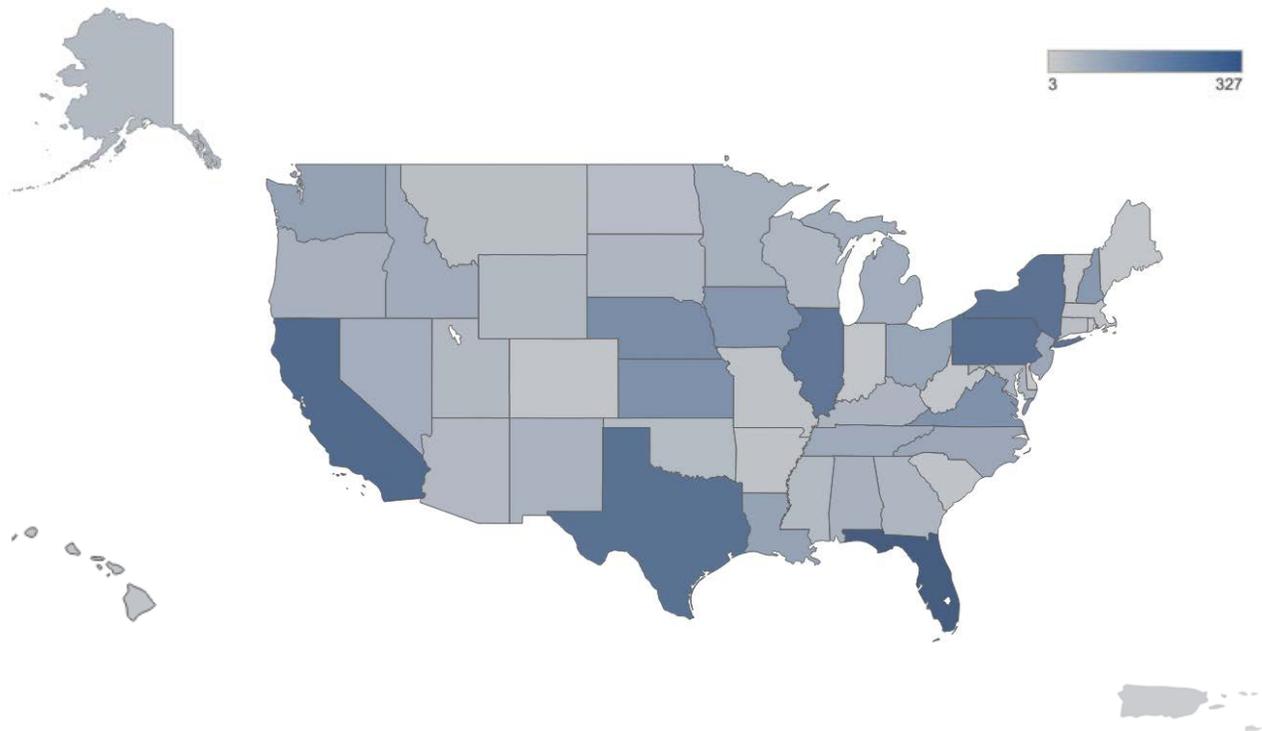


FIGURE 4.—PSA-led ISTs by State, FY 2010–FY 2016



Although some states with relatively fewer facilities and regulated sectors likely require less attention (because they are assessed in other ways), the appropriate number of facilities to assess within sectors and across geographic locations remains unclear. Also unclear is how threat and consequence factor into the “ideal” number of assessments (of any type) to conduct.

**Finding: RRAP fills a number of assessment gaps.** For example:

- **Geography:** RRAP is the only IP assessment designed to address a wider geographic scope than a single facility, function, or organization.
- **Time:** RRAP is the only assessment executed over a year or more, keeping stakeholders involved over the life of the project.
- **Scale and data quality:** A variety of participating analysts and stakeholders are working to produce unique analytical products.
- **Functional focus:** RRAP is the only assessment capable of scaling to different functional needs.
- **Multi-agency analyses:** RRAPs may lead IP to request that OCIA conduct an in-depth analysis of a topic prioritized by the stakeholders.

However, RRAPs are time-consuming to apply for and resource-intensive to complete. Furthermore, the information collected currently does not support audiences wider than the direct stakeholders and cannot be aggregated further or analyzed to identify national-level trends.

**Finding: Currently, there is no comprehensive set of descriptive statistics compiled on previously performed assessments.** Although IST and RST statistics are collected and can be compiled from data housed on IP Gateway, even more benefit might be gained if these data

informed future assessments. Similarly, information gathered when facilities decline to participate in an assessment does not appear to be used to inform outreach strategy. The quality of descriptive statistics on RRAPs is highly variable; analysts could benefit from having more RRAP-related information that can be aggregated, such as type (e.g., characterization, dependency, or hazard), primary sector, purpose, scenarios considered, or tools/models/assessments that were used or completed. Although the Industrial Control Systems Cyber Emergency Response Team compiles descriptive statistics annually for the CSET and CRR as part of its annual assessment report, the information reported is incomplete, as it does not document self-assessments completed by facilities. The belief is that critical infrastructure owners'/operators' confidentiality concerns outweigh the potential national strategic value of the data that could be collected, so DHS does not collect the self-assessment data. Consequently, there is a lack of comprehensive information about the assessments from the majority of users and customers, which minimizes the utility of the assessments to identify national-level trends.

**Finding: There is more demand for assessments than can be handled by the current field force.** Currently, there are not enough PSAs and CSAs to meet the demand for both physical and cyber assessments. At one point, CSAs were booked many months in advance to support cyber assessments, but they since have adjusted some procedures and have begun to implement a growth plan.

**Stakeholder Needs:** Table 8 outlines recommendations from the stakeholder engagement program related to Domain 2.

TABLE 8.—Recommendations for Conducting Assessments

| <b>Domain 2: Conducting Assessments</b>  |   |
|--|---|
| <b>Stakeholder Group</b>                 | <b>Recommendations</b>  |
| <b>Key IP and NPPD Stakeholders</b>      | <ul style="list-style-type: none"> <li>• Develop a formalized process to coordinate when more than one agency conducts assessments in an area or on the same site.</li> <li>• Consider multiple assessments rather than a single IST with extremely comprehensive questions.</li> <li>• The RST could use a general update, including a review of its questions and potential applications.</li> <li>• Develop a job aid for PSAs.</li> </ul> |
| <b>Federal Agencies External to NPPD</b> | <ul style="list-style-type: none"> <li>• Coordination would be improved by joint visits to sites when agencies outside of IP also conduct assessments.</li> </ul>   |

### **Domain 3: Managing Assessment Information**

The Managing Assessment Information domain includes all activities associated with controlling, protecting, and delivering assessment data. In achieving these activities, IP must maintain a secure enterprise data architecture (including proper authentication, authorization, access, and auditing of data and information) that supports operations, systems, and processes, while allowing easy access to high-quality, relationally linked data about infrastructure assets and systems.<sup>4</sup>

<sup>4</sup> This currently is managed by the IP Gateway system.

**Finding: The balance between data security and information sharing is skewed heavily toward security.** “Data security” has two primary contexts. First, data must be kept safe from those trying to acquire it for illegitimate reasons, which is a constant concern for data stored electronically. IP maintains vigilance to ensure that the data collected from assessments are secure because this capability is vital to convincing critical infrastructure owners/operators to complete assessments and allows IP to store the resulting data. Second, IP should assist data consumers in correctly interpreting and using (sharing, aggregating, analyzing, and contextualizing) assessment data. Although IP has developed products to help users to interpret data, these products have not prevented the misuse of data fully, and there were general concerns raised regarding the use of PCII and of business-sensitive information. To alleviate these concerns, IP limits access to raw data to groups that understand its meaning and limitations, and applies a low threshold for designating data as PCII. However, these actions prevent IP from sharing data more widely, potentially keeping it out of the hands of those who could conduct further analysis.

**Finding: Data management is not designed to integrate information gained through different assessments.** Although IP Gateway can and does host data from other assessments, the potential to truly integrate different datasets (i.e., to be able to combine and analyze data from the same facility in different assessments) has not been explored yet. This makes it challenging to perform analyses that require data from multiple assessment platforms, and to build a complete picture of an area’s dependencies and interdependencies. For example, though the Federal Protective Service (FPS) houses its data on IP Gateway, its information currently is not accessible to IP users on IP Gateway.

**Finding: Users and customers could get much more out of data stored on IP Gateway.** Although there are some issues around the content and quality of the data, this is, in part, because of the fact that IP Gateway is not storing assessment data in a way that is compatible with user requirements. For example:

- It is difficult to perform data searches to retrieve data;
- Not all critical infrastructure owners/operators can access their own data easily; and
- Currently, there is no easy way to access all RRAP reports in IP Gateway—a search for all RRAP reports may yield only a portion of them. Furthermore, the data from studies and assessments associated with an RRAP are not housed in IP Gateway, which limits the capabilities of IP and other organizations (such as OCIA) that might be able to conduct further analysis themselves with the data.

**Finding: There is no overarching integrated data-management strategy for critical infrastructure-related information.** There is no agencywide strategy that guides the acquisition and maintenance of data and understanding of its use. This should be coordinated across all components of NPPD that engage in assessment-related activities.

**Stakeholder Needs:** Table 9 outlines recommendations from the stakeholder engagement program related to Domain 3.

TABLE 9.—Recommendations for Managing Assessment Information

| <b>Domain 3: Managing Assessment Information</b> |  |
|--|--|
| <b>Stakeholder Group</b>                         | <b>Recommendations</b>   |
| <b>Key IP and NPPD Stakeholders</b>              | <ul style="list-style-type: none"> <li>• IT solutions across IP should be interoperable, while maintaining an optimal level of data security.</li> <li>• Data exports should be available in spreadsheet formats, in addition to PDF format.</li> <li>• The data-request process for IP Gateway can dissuade interest in using the data and would benefit from being reviewed/updated.</li> <li>• An improved ability to search in IP Gateway would increase usage.</li> <li>• The ability for users to query data directly in IP Gateway (rather than working through the labs) would increase usage of assessment data.</li> <li>• Similar data fields in different assessments across IP Gateway should be shared, while maintaining optimal levels of data security.</li> <li>• More support staff for IP Gateway would speed the ability to incorporate new users.</li> </ul> |
| <b>Federal Agencies External to NPPD</b>         | <ul style="list-style-type: none"> <li>• A reduction in the restrictions on data and reports would make the information available to a wider audience.</li> <li>• Smarter search functions in IP Gateway would encourage more usage of assessment data, so that users are able to find what they are looking for more successfully.</li> <li>• The ability to download data from IP Gateway without administrative privileges would be helpful.</li> <li>• More (and different types of) training to use IP Gateway would be helpful.</li> <li>• The ability to query answers to different questions across assessments in IP Gateway should be available to users.</li> </ul>   |

#### **Domain 4: Creating Analytic Products**

This domain includes all activities associated with enhancing the value of data through the creation and communication of findings drawn from assessment data. Achieving these activities involves identifying, acquiring, and compiling data from assessments and any other supplemental information, as well as using the data to conduct analyses. Interpretation, visualization, and communication of analysis products in ways that effectively convey relevant information to the targeted audience is also a critical component of the activities associated with this domain.

**Finding: Assessments currently do not support vulnerability analyses or the identification of broad, national mitigation strategies.** For example:

- ISTs and RSTs result in specific information that is useful to critical infrastructure owners and operators. However, the resulting data are not manipulated easily in the aggregate, preventing stakeholders with a more nationally focused mission from using the data to identify widespread areas for improvement or trends.
- Although RRAPs are regional in nature, some only involve narrowly focused analyses that address specific problems for the project sponsors. In addition, the RRAP report template does not require the inclusion of information that could be aggregated and analyzed to support mitigation at the national level. For example, type (characterization, dependency, or hazard), primary sector, purpose, scenarios considered, or

tools/models/assessments that were used or completed either are not documented or are documented in a way that does not support aggregation.

- Cyber assessments provide analytic products to those who engage in the self-assessment, but CS&C does not collect and analyze the information. Therefore CS&C's ability to analyze larger, national-level issues in the aggregate is limited.

OCIA develops planned analytic products that focus on regional or national issues, with the topics identified and prioritized by IP, CS&C, FPS, Office of Biometric Identity Management, and NPPD leadership. OCIA's ad hoc analyses are based on requirements related to emerging threats and conditions, frequently responding to questions from IP, CS&C, FPS, and NPPD leadership; or from other critical infrastructure stakeholders received through the National Infrastructure Coordinating Center or the National Cybersecurity and Communications Integration Center (although sometimes directly from other agencies, the White House, or Congress). In addition, OCIA's primary analytic approach is the prediction or approximation of the outcomes of events, rather than the examination and description of vulnerabilities. OCIA's use of infrastructure structural, operational, or systems vulnerability information is often more generalized, sometimes imbedded in its modelling workflow and used in proactive studies. In the case of analyses in a crisis action response mode, vulnerability typically is known because the incident has happened. In an emerging threat, where it would be useful for OCIA to understand the specific vulnerabilities of infrastructure in light of the specific threat, it is not currently feasible to use IP's collected information because the information typically is not formulated to be included in rapid analytic workflows effectively, and is not shared systematically so that OCIA could reformat it for such use.

**Finding: There is a need for a formalized process allowing OCIA to fill stakeholder requests for analyses that includes participation from IP and other key stakeholders.** There is a need for OCIA to formalize the process of building the NPPD analytic agenda and the roles of different partner agencies in that process, including IP. OCIA would benefit from clarifying the process so that partners can participate more efficiently and effectively. IP then could identify what types of analyses that it wants to perform, and could participate as both a contributor of requirements and as a recipient of requirements in formulating the analytic agenda. This would help both IP and OCIA to understand and organize responses to external stakeholder requirements. It also would identify a body of analytic requirements for which IP does not need OCIA's assistance, and would give OCIA the opportunity to define what modifications to IP practices could be made that would benefit OCIA's analytic capabilities and responsiveness. These types of changes would increase collaboration within NPPD and extend the governance processes for identifying and prioritizing analytic projects, including IP's.

In addition, internal factors largely determine the design and formatting of visuals (e.g., staff skillset and available tools), rather than external stakeholder requirements. Individuals are assigned to develop analytical products in an inconsistent manner and sometimes are unfamiliar with the data and objectives behind the stakeholder requests. IP can address basic analytic questions quickly if it happens to use data that already have been collected and are available in an accessible format, but analysts have had difficulties being responsive to stakeholder requests for new or more complex analysis products. This issue is exacerbated when IP is asked to

support emerging needs during a real-world response, especially for products that previously have not been requested.

**Stakeholder Needs:** Table 10 outlines recommendations from the stakeholder engagement program related to Domain 4.

TABLE 10.–Recommendations for Conducting Assessments

| Domain 4: Conducting Assessments  |   |
|-----------------------------------|---|
| Stakeholder Group                 | Recommendations   |
| Key IP and NPPD Stakeholders      | <ul style="list-style-type: none"> <li>Formalize roles of analysts from IP, OCIA, and the National Labs.</li> <li>Increase coordination between OCIA and IP divisions.</li> <li>Maintain a single analytic agenda for all of NPPD.</li> </ul> |
| Federal Agencies External to NPPD | <ul style="list-style-type: none"> <li>If an agency is included, it should be able to review the products while they are still under development.</li> </ul>  |

### Domain 5: Managing Data Quality

This domain includes all activities associated with ensuring that the data collected from assessments are suitable for its intended purpose. Accomplishing these activities involves establishing data-quality levels for critical data; conducting assessments and tracking activities that support identification of data-quality issues; and developing corrective actions to improve data quality.

**Finding: There are multiple mechanisms for monitoring and evaluating IST and RST data.** Both the IST and the RST are designed such that assessors (either through facilitation or through self-assessment) complete all questions. This ensures complete data sets and allows for more valid aggregation of assessment information. There are several additional processes for ensuring data quality for PSA-led assessments:

1. There are algorithms that check for general anomalies, such as when questions are skipped or when responses do not align to overall trends.
2. A team of personnel at both IP headquarters and Argonne National Laboratory review the data for accuracy, completeness, and consistency, and can raise questions for the PSAs, as needed.
3. Critical infrastructure owners/operators and PSAs have the opportunity to identify and address mistakes, although the system to do so could be clearer.

For self-assessments, however, only the first process occurs.

**Finding: There are limited processes to ensure continual improvement of data quality.** Although the processes noted above flag possible issues with accuracy, completeness, and consistency, IP does not have formal processes to support continual improvement. For example, corrections are not logged or analyzed to determine trends or root causes of errors. Furthermore, although the Infrastructure Information Collection Division does review annual assessment requirements to provide an opportunity for stakeholders to offer suggestions for improving assessments, there are no formal structures or processes in place to elicit feedback from data

users and customers to improve data quality or to determine if there are unmet requirements from potential customers. In addition, although monitoring occurs in accordance with data-quality parameters, outcomes from monitoring are not communicated specifically to relevant parties (e.g., assessor, assessor’s supervisor) or used to improve data quality. As data age, there is no formal mechanism to check data currency and/or accuracy.

**Finding: Automation of Quality Assurance/Quality Control (QA/QC) processes could increase efficiency.** Currently, IP does not have automated QA/QC processes for the bulk of its data-validation requirements for assessments. Some assessments have built in the capability to check for some variances, but most quality assurance requires a hands-on review by analysts. Although there are generally enough QA/QC staff for normal, day-to-day requirements, the limited automation strains resources during surges (e.g., at the end of the fiscal year). This issue is exacerbated further by a lack of formal processes to surge new resources quickly.

**Finding: Formalized data-quality criteria do not exist for all assessments.** IP has identified a core set of data-quality objectives—such as targets, thresholds, and metrics—for some assessments, such as the IST. However, IP does not weigh the strategic importance of the data elements. As a result, the level of effort that goes into monitoring data-quality criteria currently may not be aligned with strategic requirements. IP and CS&C should consider the impact of data quality on downstream decisions (e.g., decisions about planning, response efforts) when developing quality criteria, in order to ensure that data-quality resources are focused on the most critical data elements.

**Stakeholder Needs:** Table 11 outlines recommendations from the stakeholder engagement program related to Domain 5.

TABLE 11.—Recommendations for Managing Data Quality

| <b>Domain 5: Managing Data Quality</b> |   |
|--|---|
| <b>Stakeholder Group</b>               | <b>Recommendations</b>  |
| <b>Key IP and NPPD Stakeholders</b>    | <ul style="list-style-type: none"> <li>• IP should identify which questions are more critical than others and should determine the appropriate level of corresponding QA, which may differ from one question to another.</li> <li>• The QA process might benefit from a more centralized organizational structure; because it is the dedicated task of a few staff and there is no single program leader, it can get deprioritized easily.</li> <li>• An automated weekly reminder to QA staff when they have QA tasks waiting would improve timeliness of the QA process.</li> <li>• More detailed (i.e., more digits) and more accurate geocodes are needed to improve data quality.</li> </ul> |

## Appendix C: The Strategic Planning Process

