September 2014

# CRITICAL INFRASTRUCTURE PROTECTION

## DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts

GAO Highlights

Highlights of GAO-14-507, a report to congressional requesters

### Why GAO Did This Study

Damage from natural disasters like Hurricane Sandy in 2012 highlights the vulnerability of the nation's CI. CI includes assets and systems whose destruction would have a debilitating effect on security, national economic security, or national public health or safety. The private sector owns the majority of the nation's CI, and multiple federal entities, including DHS, are involved in assessing its vulnerabilities. These assessments can identify factors that render an asset or facility susceptible to threats and hazards. GAO was asked to review how federal entities assess vulnerabilities.

This report examines the extent to which DHS is positioned to (1) integrate DHS vulnerability assessments to identify priorities, (2) identify duplication and gaps within its coverage, and (3) manage an integrated and coordinated government-wide assessment approach. GAO reviewed CI laws, regulations, data from fiscal years 2011-2013, and other related documentation, as well as interviewed officials at DHS, other agencies, and a private CI association.

### What GAO Recommends

GAO recommends that DHS identify the areas assessed for vulnerability most important for integrating and comparing results, establish guidance for DHS offices and components to incorporate these areas into their assessments, ensure that assessment data are consistently collected, and work with other federal entities to develop guidance for what areas to include in vulnerability assessments, among other things. DHS concurred with these recommendations.

View GAO-14-507. For more information, contact Stephen Caldwell at (202) 512-8777 or caldwells@gao.gov.

### What GAO Found

During fiscal years 2011 to 2013, various Department of Homeland Security (DHS) offices and components conducted or required thousands of vulnerability assessments of critical infrastructure (CI), but DHS is not positioned to integrate them in order to identify priorities. Although the Homeland Security Act of 2002 and the *National Infrastructure Protection Plan* (NIPP) call for DHS to integrate CI vulnerability assessments to identify priorities, the department cannot do so because of variation in the areas to be assessed for vulnerability included in the various tools and methods used by DHS. GAO analysis of 10 of these assessment tools and methods found that they consistently included some areas, such as perimeter security, but other areas, such as cybersecurity, were not consistently included in the 10 tools and methods. Also, GAO's analysis and discussions with DHS officials showed that DHS's assessments vary in their length and detail of information collected, and DHS has not established guidance on what areas should be included in a vulnerability assessment, such as vulnerabilities to all-hazards as called for in the NIPP. DHS's Office of Infrastructure Protection (IP) has recognized the challenge of having different approaches and has begun to take action to harmonize them. However, of the 10 assessment tools and methods GAO analyzed, IP's harmonization effort includes two voluntary IP assessment tools and none of the other 8 tools and methods GAO analyzed that are used by other DHS offices and components. By reviewing the tools and methods to identify the areas of vulnerability and level of detail that DHS considers necessary, and establishing guidance for DHS offices and components regarding which areas to include in their assessments, DHS would be better positioned to integrate assessments to enable comparisons and determine priorities between and across CI sectors.

DHS offices and components have not consistently captured and maintained data on vulnerability assessment activities in a way that allows DHS to identify potential duplication or overlap in coverage among vulnerability assessment activities they have conducted or required. As a result, DHS is not positioned to track its activities to determine whether its assessment efforts are potentially duplicative or leave gaps among the CI assessed and thereby better ensure effective risk management across the spectrum of assets and systems, as called for by the NIPP. Developing an approach to collect data consistently would facilitate DHS's identification of potential duplication or overlap in CI coverage. Having consistent data would also better position DHS to minimize the fatigue CI owners expressed experiencing from participation in multiple assessments.

DHS is not positioned to manage an integrated and coordinated government-wide approach for assessments as called for in the NIPP because it does not have sufficient information about the assessment tools and methods conducted or offered by federal entities external to DHS with CI responsibilities, such as the Environmental Protection Agency, which oversees critical infrastructure activities related to water and wastewater systems. Consequently, opportunities exist for DHS to work with other federal entities to develop guidance as necessary to ensure consistency. Doing so would better position DHS and other federal entities with CI responsibilities to promote an integrated and coordinated approach for conducting vulnerability assessments of CI, as called for in the Homeland Security Act of 2002, presidential directives, and the NIPP.