October 2017

CRITICAL INFRASTRUCTURE PROTECTION

DHS Risk Assessments Inform Owner and Operator Protection Efforts and Departmental Strategic Planning

GAO Highlights

Highlights of GAO-18-62, a report to congressional requesters

Why GAO Did This Study

The nation's critical infrastructure includes cyber and physical assets and systems across 16 different sectors whose security and resilience are vital to the nation. The majority of critical infrastructure is owned and operated by the private sector. Multiple federal entities, including DHS, work with infrastructure owners and operators to assess their risks.

GAO was asked to review DHS's risk assessment practices for critical infrastructure. This report describes:(1) DHS's risk assessment practices in 3 of 16 critical infrastructure sectors and private sector representatives' views on the utility of this risk information, and (2) how this risk information influences DHS's strategic planning and private sector outreach.

GAO selected 3 of 16 sectors–Critical Manufacturing; Nuclear Reactors, Materials, and Waste; and Transportation Systems–to examine based on their varied regulatory structures and industries. GAO reviewed DHS guidance related to infrastructure protection, the QHSR and DHS Strategic Plan, and plans for the selected critical infrastructure sectors. GAO interviewed DHS officials responsible for critical infrastructure risk assessments, and the owner and operator representatives who serve as chairs and vice-chairs of coordinating councils for the 3 selected sectors. Information from the 3 sectors is not generalizable to all 16 sectors but provides insight into DHS's risk management practices.

GAO provided a draft of this report to DHS and relevant excerpts to the council representatives interviewed during this review. Technical comments provided were incorporated as appropriate.

View GAO-18-62. For more information, contact Chris Currie at (404) 679-1875 or curriec@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) primarily conducts assessments for each of the three elements of risk—threat, vulnerability, and consequence—for critical infrastructures from the three sectors GAO reviewed—Critical Manufacturing; Nuclear Reactors, Materials, and Waste; and Transportation Systems. In limited circumstances, DHS generates risk assessments that both incorporate all three elements of risk and cover individual or multiple subsectors.

- **Threat**: DHS's Office of Intelligence and Analysis assesses threats—natural or manmade occurrences, entities, or actions with the potential to cause harm, including terrorist attacks and cyberattacks—and disseminates this information to critical infrastructure owners and operators. For example, the Transportation Security Administration provides threat intelligence to mass transit security directors and others through joint classified briefings.
- **Vulnerability:** DHS officials provide various tools and work directly with owners and operators to assess asset and facility vulnerabilities—physical features or operational attributes that render an asset open to exploitation, including gates, perimeter fences, and computer networks. For example, DHS officials conduct voluntary, asset-specific vulnerability assessments that focus on physical infrastructure during individual site visits.
- **Consequence:** DHS officials also assess consequence— the effect of occurrences like terrorist attacks or hurricanes resulting in losses that impact areas such as public health and safety, and the economy—to better understand the effect of these disruptions on assets.

These assessments help critical infrastructure owners and operators take actions to improve security and mitigate risks. Six private sector representatives told GAO that threat information is the most useful type of risk information because it allows owners and operators to react immediately to improve their security posture. For example, one official from the Transportation Systems sector said that government threat information is credible and is critical in supporting security recommendations to company decision-makers.

DHS uses the results of its risk assessments to inform the department's strategic planning and to guide outreach to infrastructure owners and operators. Critical infrastructure risk information is considered within DHS's strategic planning. Specifically, according to DHS officials, risk information informs the Department's Quadrennial Homeland Security Review (QHSR)—a process that identifies DHS's critical homeland security missions and its strategy for meeting them. DHS also uses risk information to guide outreach to critical infrastructure owners and operators. For example, DHS officials annually prioritize the most critical assets and facilities nationwide and categorize them based on the severity of the estimated consequences of a significant disruption to the asset or facility. DHS officials then use the results to target their assessment outreach to the infrastructure owners and operators categorized as higher risk. DHS officials also told GAO that they use risk information after an incident, such as a natural disaster, to quickly identify and prioritize affected infrastructure owners and operators to help focus their response and recovery assistance outreach.