February 2017

CRITICAL INFRASTRUCTURE PROTECTION

Additional Actions by DHS Could Help Identify Opportunities to Harmonize Access Control Efforts

GAO Highlights

Highlights of GAO-17-182, a report to congressional committees

Why GAO Did This Study

Critical infrastructure protection access controls limit access to those with a legitimate need. DHS is the lead federal agency for coordinating critical infrastructure protection efforts with other federal agencies, and partnering with nonfederal stakeholders. The National Defense Authorization Act of 2016 included a provision for GAO to review critical infrastructure access control efforts.

This report examines (1) key characteristics of selected federally-administered critical infrastructure access control efforts and factors that have an impact on stakeholders' use of them; (2) the extent to which DHS has taken actions to harmonize efforts across critical infrastructure sectors; and (3) the extent to which DHS's SCO has taken actions to harmonize access control efforts across DHS. GAO examined six federally-administered access control efforts across three federal departments. Efforts were selected, among other things, to represent a range of efforts that groups of users—such as truck drivers—may encounter while accessing multiple facilities. GAO interviewed DHS, NRC, and DOD officials and users and operators affected by the efforts and reviewed relevant documents.

What GAO Recommends

GAO recommends that (1) DHS work with partners to identify any opportunities to harmonize access control efforts across critical infrastructure sectors and (2) SCO establish goals and objectives to support its broader strategic framework for harmonization. DHS concurred with both recommendations.

View GAO-17-182. For more information, contact Chris P. Currie at (404) 679-1875 or CurrieC@gao.gov.

What GAO Found

The six selected federally-administered critical infrastructure access control efforts GAO reviewed generally followed similar screening and credentialing processes. Each of these efforts applies to a different type of infrastructure. For example, the Transportation Security Administration's Transportation Worker Identification Credential controls access to ports, the Department of Defense (DOD) Common Access Card controls access to military installations, and the Nuclear Regulatory Commission (NRC) regulates access to commercial nuclear power plants. GAO found that selected characteristics, such as whether a federal agency or another party has responsibility for vetting or what types of prior criminal offenses might disqualify applicants, varied across these access control efforts. In addition, these access control efforts generally affect two groups of stakeholders—users and operators—differently depending on their specific roles and interests. Users are individuals who require access to critical infrastructure as an essential function of their job; while, operators own or manage facilities, such as airports and chemical facilities. Regardless of infrastructure type, users and operators that GAO interviewed reported some common factors that can present challenges in their use of these access controls. For example, both users and operators reported that applicants requiring access to similar types of infrastructure or facilities may be required to submit the same background information multiple times, which can be costly and inefficient.

The Department of Homeland Security (DHS) relies on partnership models to support collaboration efforts among federal and nonfederal critical infrastructure stakeholders, but has not taken actions to harmonize federally-administered access control efforts across critical infrastructure sectors. According to DHS officials, these partnerships have not explored harmonization of access control efforts across sectors, because this has not been raised as a key issue by the members and because DHS does not have a dedicated forum that would engage user groups in exploring these issues and identifying potential solutions. DHS's partnership models offer a mechanism by which DHS and its partners can explore the challenges users and operators may encounter and determine opportunities for harmonizing the screening and credentialing processes to address these challenges.

DHS's Screening Coordination Office (SCO) has taken actions to support harmonization across DHS access control efforts, but it has not updated its goals and objectives to help guide progress toward the department's broader strategic framework for harmonization. SCO's strategic framework is based on two screening and credentialing policy documents—the 2006 Credentialing Initiative Report and 2008 Credentialing Framework Initiative. According to SCO officials, they continue to rely on these documents to provide their office with a high-level strategic approach, but GAO found that the goals and objectives outlined in the two documents are no longer current or relevant. In recent years, SCO has helped the department make progress toward its harmonization efforts by responding to and assisting with department-wide initiatives and DHS component needs, such as developing new programs or restructuring existing ones. However, without updated goals and objectives, SCO cannot ensure that it is best supporting DHS-wide screening and credentialing harmonization efforts.