GAO Highlights

Highlights of GAO-20-453, a report to congressional requesters

May 2020

CRITICAL INFRASTRUCTURE PROTECTION

Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities

Why GAO Did This Study

Thousands of high-risk chemical facilities may be subject to the risk posed by cyber threat adversaries—terrorists, criminals, or nations. These adversaries could potentially manipulate facilities' information and control systems to release or steal hazardous chemicals and inflict mass causalities to surrounding populations (see figure). In accordance with the DHS Appropriations Act, 2007, DHS established the CFATS program to, among other things, identify and assess the security risk posed to chemical facilities.

GAO was asked to examine the cybersecurity efforts of the CFATS program, including the extent to which the program (1) assesses the cybersecurity efforts of covered facilities, and (2) determines the specialty training and level of staff needed to assess cybersecurity at covered facilities.

GAO conducted site visits to observe the cybersecurity portion of CFATS inspections based on scheduled inspections, reviewed inspection documents, and interviewed CFATS inspectors. GAO also analyzed inspection guidance and training against key practices and assessed workforce planning documents and processes.

What GAO Recommends

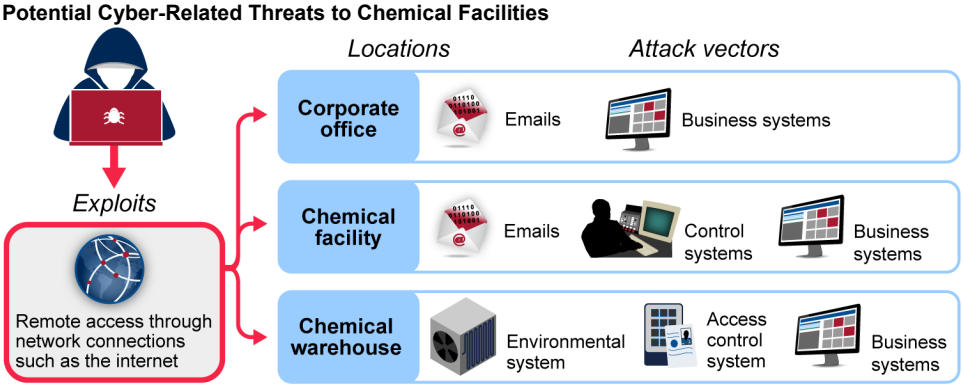
GAO is making six recommendations to DHS to routinely review guidance and update, as needed; to fully incorporate key training practices; and to identify workforce cybersecurity needs. DHS concurred with the recommendations.

View GAO-20-453. For more information, contact Nathan Anderson at (206) 287-4804 or andersonn@gao.gov or Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

The Chemical Facility Anti-Terrorism Standards (CFATS) program within the Department of Homeland Security (DHS) evaluates high-risk chemical facilities' cybersecurity efforts via inspections that include reviewing policies and procedures, interviewing relevant officials, and verifying facilities' implementation of agreed-upon security measures. GAO found that the CFATS program has guidance designed to help the estimated 3,300 CFATS-covered facilities comply with cybersecurity and other standards, but the guidance has not been updated in more than 10 years, in contrast with internal control standards which recommend periodic review. CFATS officials stated that the program does not have a process to routinely review its cybersecurity guidance to ensure that it is up to date with current threats and technological advances. Without such a process, facilities could be more vulnerable to cyber-related threats.

Potential Cyber-Related Threats to Chemical Facilities



Source: GAO analysis of potential cybersecurity threats to chemical facilities. | GAO-20-453

The CFATS program developed and provided cybersecurity training for its inspectors, but GAO found that the CFATS program does not fully address 3 of 4 key training practices, or address cybersecurity needs in its workforce planning process, as recommended by DHS guidance. Specifically:

- The CFATS program does not: (1) systematically collect or track data related to inspectors' cybersecurity training or knowledge, skills, and abilities; (2) develop measures to assess how training is contributing to cybersecurity-related program results; or (3) have a process to evaluate the effectiveness of its cybersecurity training in improving inspector skillsets.
- The program also has yet to incorporate identified cybersecurity knowledge, skills, and abilities for inspectors in its current workforce planning processes or track data related to covered facilities' reliance on information systems when assessing its workforce needs.

Fully addressing key training practices will help ensure that CFATS inspectors have the knowledge, skills, and abilities for cybersecurity inspections, and identifying cybersecurity needs in workforce planning will help the program ensure that it has the appropriate number of staff to carry out the program's cybersecurity-related efforts.