CRITICAL INFRASTRUCTURE PROTECTION

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

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

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.