January 2024

CRITICAL INFRASTRUCTURE PROTECTION

Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support

GAO Highlights

Highlights of GAO-24-106221, a report to congressional addressees

Why GAO Did This Study

The nation's 16 critical infrastructure sectors provide essential services such as electricity, healthcare, and gas and oil distribution. However, cyber threats to critical infrastructure, such as ransomware, represent a significant national security challenge.

This report (1) describes the reported impact of ransomware attacks on the nation's critical infrastructure, (2) assesses federal agency efforts to oversee sector adoption of leading federal practices, and (3) evaluates federal agency efforts to assess ransomware risks and the effectiveness of related support.

To do so, GAO selected four critical infrastructure sectors—critical manufacturing, energy, healthcare and public health, and transportation systems. For each sector, GAO analyzed documentation, such as incident reporting and risk analysis, and compared efforts to leading cybersecurity guidance. GAO also interviewed sector and federal agency officials to obtain information on ransomware-related impacts, practices, and support.

What GAO Recommends

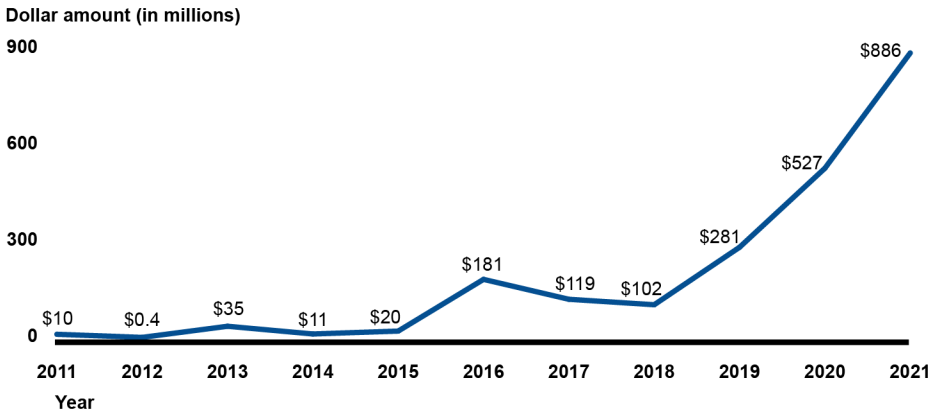
GAO is making 11 recommendations to four agencies to, among other things, determine selected sectors' adoption of cybersecurity practices. DHS and HHS agreed with their recommendations. DOE partially agreed with one recommendation and disagreed with another. DOT agreed with one recommendation, partially agreed with one, and disagreed with a third. GAO continues to believe that the recommendations are valid.

View GAO-24-106221. For more information, contact David B. Hinchman at (214) 777-5719 or HinchmanD@gao.gov.

What GAO Found

Ransomware—software that makes data and systems unusable unless ransom payments are made—is having increasingly devastating impacts. For example, the Department of the Treasury reported that the total value of U.S. ransomware-related incidents reached $886 million in 2021, a 68 percent increase compared to 2020 (see figure).

Treasury Reported Dollar Value of U.S. Ransomware-Related Incidents



Source: GAO analysis of Department of the Treasury data. | GAO-24-106221

In addition to monetary losses, ransomware has led to other impacts, such as the inability to provide emergency care when hospital IT systems are unusable. The FBI reported that 870 critical infrastructure organizations were victims of ransomware in 2022, affecting 14 of the 16 critical infrastructure sectors. Among those incidents, almost half were from four sectors—critical manufacturing, energy, healthcare and public health, and transportation systems. The full impact of ransomware is likely not known because reporting is generally voluntary. The Department of Homeland Security is planning to issue new reporting rules by March 2024 that could provide a more complete picture of ransomware's impact.

The four selected sectors' adoption of leading practices to address ransomware is largely unknown. None of the federal agencies designated as the lead for risk management for selected sectors have determined the extent of adoption of the National Institute of Standards and Technology's recommended practices for addressing ransomware. Doing so would help the lead federal agencies be a more effective partner in national efforts to combat ransomware.

Most of the six selected lead federal agencies have assessed or plan to assess risks of cybersecurity threats including ransomware for their respective sectors, as required by law. Regarding lead agencies assessing their support of sector efforts to address ransomware, half of the agencies have evaluated aspects of their support. For example, agencies have received and assessed feedback on their ransomware guidance and briefings. However, none have fully assessed the effectiveness of their support to sectors, as recommended by the National Infrastructure Protection Plan. Fully assessing effectiveness could help address sector concerns about agency communication, coordination, and timely sharing of threat and incident information.