GAO Highlights

Highlights of GAO-18-645T, a testimony before the Subcommittees on Government Operations and Information Technology, Committee on Oversight and Government Reform, House of Representatives

July 2018

HIGH-RISK SERIES

Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation

Why GAO Did This Study

Federal agencies and the nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on information technology systems to carry out operations. The security of these systems and the data they use is vital to public confidence and national security, prosperity, and well-being.

The risks to these systems are increasing as security threats evolve and become more sophisticated. GAO first designated information security as a government-wide high-risk area in 1997. This was expanded to include protecting cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.

GAO was asked to update its information security high-risk area. To do so, GAO identified the actions the federal government and other entities need to take to address cybersecurity challenges. GAO primarily reviewed prior work issued since the start of fiscal year 2016 related to privacy, critical federal functions, and cybersecurity incidents, among other areas. GAO also reviewed recent cybersecurity policy and strategy documents, as well as information security industry reports of recent cyberattacks and security breaches.

What GAO Recommends

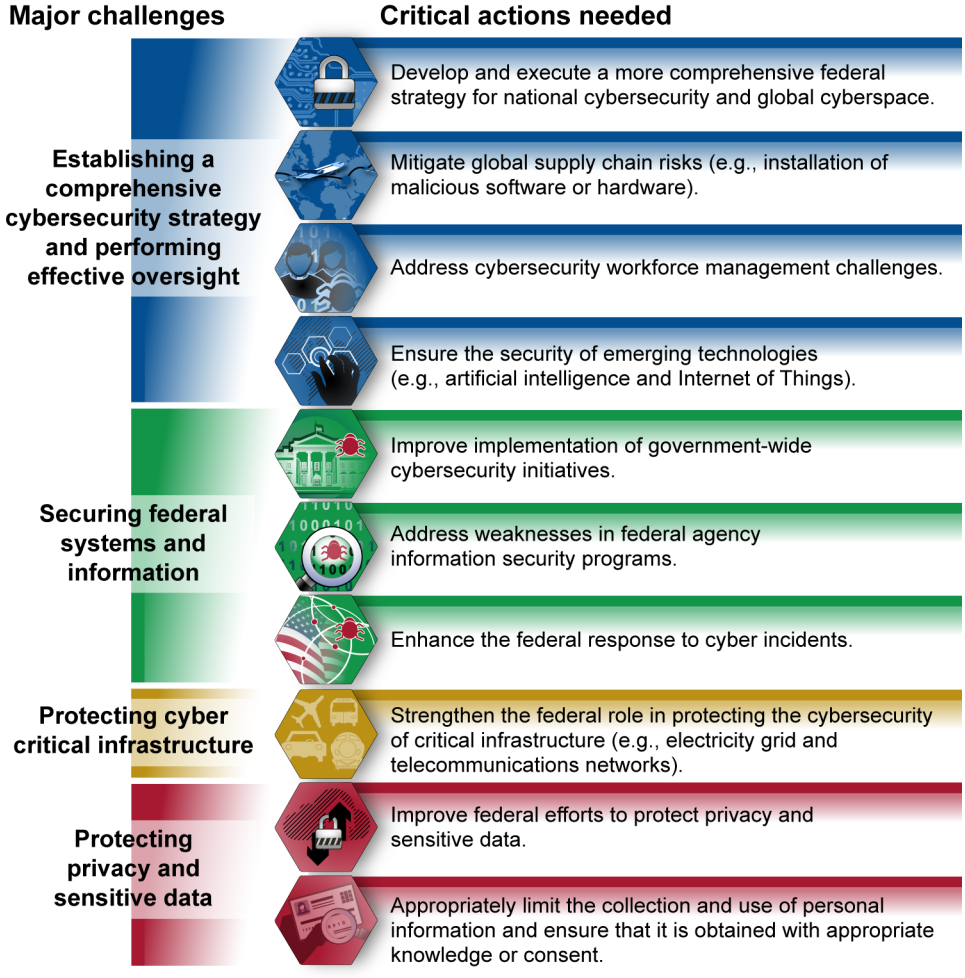
GAO has made over 3,000 recommendations to agencies since 2010 aimed at addressing cybersecurity shortcomings. As of July 2018, about 1,000 still needed to be implemented.

View GAO-18-645T. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

GAO has identified four major cybersecurity challenges and 10 critical actions that the federal government and other entities need to take to address them. GAO continues to designate information security as a government-wide high-risk area due to increasing cyber-based threats and the persistent nature of security vulnerabilities.

Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges



Source: GAO analysis. | GAO-18-645T

GAO has made over 3,000 recommendations to agencies aimed at addressing cybersecurity shortcomings in each of these action areas, including protecting cyber critical infrastructure, managing the cybersecurity workforce, and responding to cybersecurity incidents. Although many recommendations have been addressed, about 1,000 have not yet been implemented. Until these shortcomings are addressed, federal agencies' information and systems will be increasingly susceptible to the multitude of cyber-related threats that exist.