

GAO Highlights

Highlights of [GAO-24-106916](#), a report to congressional addressees

Why GAO Did This Study

For over 25 years GAO has identified cybersecurity as a high-risk area. During this period, the threat of cyber-based intrusions and attacks on IT systems by malicious actors has continued to grow.

A national strategy to guide the government's cybersecurity activities is needed to address this threat. Recognizing the need for national cybersecurity leadership, Congress established ONCD to support the nation's cybersecurity and lead the development of a national strategy. In March 2023, the White House issued the *National Cybersecurity Strategy* to outline how the administration will manage the nation's cybersecurity. In July 2023, ONCD issued an implementation plan defining how the strategy will be executed.

GAO's objective was to examine the extent to which the *National Cybersecurity Strategy* and implementation plan addressed desirable characteristics of a national strategy. To do so, GAO assessed relevant documents and other evidence against desirable characteristics of a national strategy. GAO also interviewed ONCD staff.

What GAO Recommends

GAO is making two recommendations to ONCD to develop outcome-oriented measures and estimate costs of implementation activities. ONCD agreed with GAO's recommendation on outcome-oriented measures but disagreed with the recommendation on estimating costs. GAO continues to believe that ONCD should assess the plan's initiatives to identify those that warrant a cost estimate and develop such cost estimates.

View [GAO-24-106916](#). For more information, contact Marisol Cruz Cain at (202) 512-5017 or CruzCainM@gao.gov

February 2024

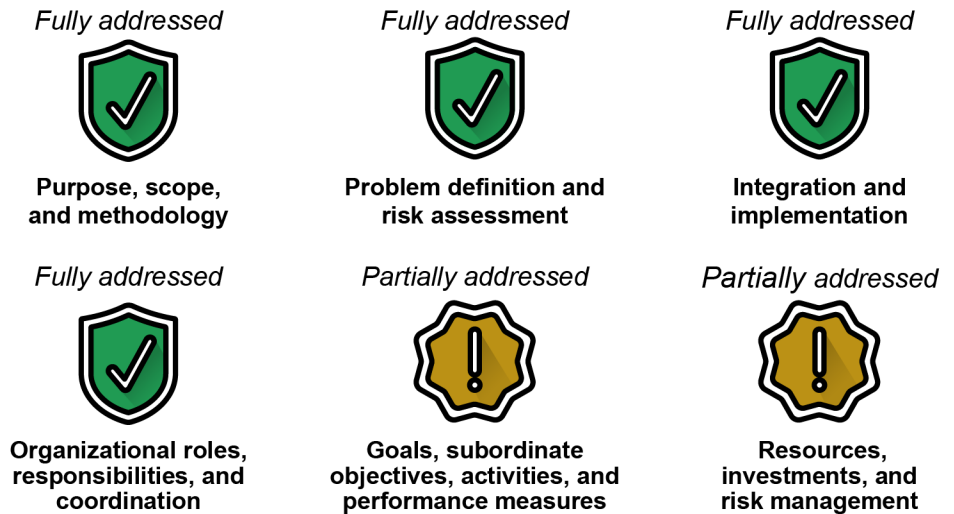
CYBERSECURITY

National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy

What GAO Found

The *National Cybersecurity Strategy* and its implementation plan jointly addressed four of six desirable characteristics identified in prior GAO work and partially addressed the other two (see figure).

Extent to Which the March 2023 *National Cybersecurity Strategy* and July 2023 Implementation Plan Addressed GAO's Desirable Characteristics of a National Strategy



Source: GAO analysis and icon; yevheniia/stock.adobe.com (icons). | GAO-24-106916

For the partially addressed characteristics, the documents did not fully describe:

- **Outcome-oriented performance measures.** Office of the National Cyber Director (ONCD) staff said it was not realistic to develop outcome-oriented measures at this point. However, GAO believes it is feasible to develop such measures where applicable. For example, regarding the key initiative of disrupting ransomware attempts, the Department of the Treasury already collects information on the number and dollar value of ransomware-related incidents—for 2021 the reported total dollar value was about \$886 million. This demonstrates that developing such measures is feasible and can be used for measuring effectiveness.
- **Resources and estimated costs.** While the implementation plan outlined initiatives that require executive visibility and interagency coordination, it did not identify how much it will cost to implement the initiatives. ONCD staff said estimating the cost to implement the entire strategy was unrealistic. However, while certain initiatives may not warrant a specific cost estimate, other activities supporting some of the key initiatives with potentially significant costs justify the development of a cost estimate. Such cost estimates are essential to effectively managing programs. Without such information, uncertainty can emerge about investing in programs.

Without actions to address these shortcomings, ONCD will likely lack information on plan outcomes and encounter uncertainty on funding of activities.