GAO Highlights

Highlights of GAO-24-106624, a report to congressional requesters

May 2024

NASA CYBERSECURITY

Plan Needed to Update Spacecraft Acquisition Policies and Standards

Why GAO Did This Study

NASA's space development project portfolio includes 34 major projects, in which NASA plans to invest more than $83 billion. Spacecraft are operating in a heightened cyber threat environment with increased risks of attack and mission disruption. NASA has identified civil space events that demonstrate the need to better protect spacecraft against cyber threats.

GAO was asked to examine the cybersecurity requirements in NASA contracts for its spacecraft projects. This report assesses the extent to which NASA (1) incorporated cybersecurity in selected spacecraft contracts and (2) determined whether additional cybersecurity updates, if any, are needed to its acquisition policies and standards for spacecraft.

GAO reviewed NASA policies and standards regarding spacecraft cybersecurity. GAO selected a nongeneralizable sample of three spacecraft projects, chosen because they represent different NASA centers and development stages, and include at least one robotic and one human spaceflight project. For these three, GAO analyzed contracts and project documents. GAO also interviewed project and cybersecurity officials.

What GAO Recommends

GAO recommends NASA develop a plan with time frames to update its spacecraft acquisition policies to include essential controls. NASA agreed to update its policies but did not agree to set a plan with dates to do so. Without a plan, GAO maintains it is unknown when implementation would occur. Accordingly, the recommendation remains valid.

View GAO-24-106624. For more information, contact W. William Russell at (202) 512-4841 or russellw@gao.gov, or Kevin Walsh at (202) 512-6151 or walshk@gao.gov.

What GAO Found

Spacecraft developed by the National Aeronautics and Space Administration (NASA) depend on software and IT, which, in turn, rely on cybersecurity to prevent, detect, and respond to potential cyber incidents. A cyber incident could result in loss of mission data, decreased lifespan or capability of space systems, or the loss of control of space vehicles. Cyber threats and technology change rapidly. In response, the federal government issues government-wide cybersecurity guidelines, such as the National Institute of Standards and Technology's Risk Management Framework.

Source: KanawatTH/stock.adobe.com. | GAO-24-106624

Contracts for the selected NASA projects GAO reviewed required contractors to address cybersecurity, consistent with NASA standards. In 2019, NASA identified a set of cybersecurity requirements for spacecraft to address. For example, NASA requires spacecraft to protect positioning, navigation, and timing systems. The three spacecraft projects GAO reviewed—Gateway Power and Propulsion Element; Orion Multi-Purpose Crew Vehicle; and Spectro-Photometer for the History of the Universe, Epoch of Re-ionization and Ices Explorer—started development before 2019. Nevertheless, GAO found these contracts include requirements related to NASA's spacecraft cybersecurity standards. Contracts also required contractors to demonstrate requirements are met through testing.

Since the issuance of its 2019 cybersecurity requirements, NASA has considered, but not yet implemented, updates to its spacecraft acquisition policies and standards. In 2023, NASA issued a space best practices guide containing information on cybersecurity principles and controls, threat actor capabilities, and potential mitigation strategies, among other things. However, this guidance is optional for spacecraft programs. NASA officials explained that one key reason they have not yet incorporated this guidance into required acquisition policies and standards is because of the length of time it takes to do so. GAO acknowledges that the standards-setting process can take time, but it is essential that NASA do so for practices that should be required. However, officials stated that they did not have an implementation plan and time frame to incorporate additional security controls into acquisition policies and standards. As a result, NASA risks inconsistent implementation of cybersecurity controls and lacks assurance that spacecraft have a layered and comprehensive defense against attacks.