GAO Highlights

Highlights of GAO-19-128, a report to the Committee on Armed Services, U.S. Senate

Why GAO Did This Study

DOD plans to spend about $1.66 trillion to develop its current portfolio of major weapon systems. Potential adversaries have developed advanced cyber-espionage and cyber-attack capabilities that target DOD systems. Cybersecurity—the process of protecting information and information systems—can reduce the likelihood that attackers are able to access our systems and limit the damage if they do.

GAO was asked to review the state of DOD weapon systems cybersecurity. This report addresses (1) factors that contribute to the current state of DOD weapon systems' cybersecurity, (2) vulnerabilities in weapons that are under development, and (3) steps DOD is taking to develop more cyber resilient weapon systems.

To do this work, GAO analyzed weapon systems cybersecurity test reports, policies, and guidance. GAO interviewed officials from key defense organizations with weapon systems cybersecurity responsibilities as well as program officials from a non-generalizable sample of nine major defense acquisition program offices.

What GAO Recommends

GAO is not making any recommendations at this time. GAO will continue to evaluate this issue.

View GAO-19-128. For more information, contact Cristina Chaplain, 202-512-4841, chaplainc@gao.gov

October 2018

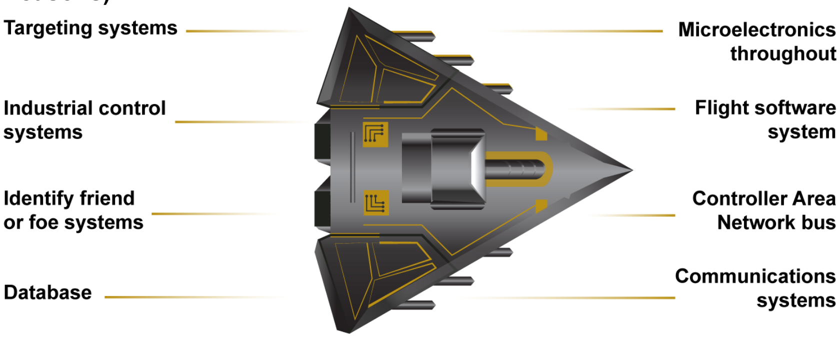
WEAPON SYSTEMS CYBERSECURITY

DOD Just Beginning to Grapple with Scale of Vulnerabilities

What GAO Found

The Department of Defense (DOD) faces mounting challenges in protecting its weapon systems from increasingly sophisticated cyber threats. This state is due to the computerized nature of weapon systems; DOD's late start in prioritizing weapon systems cybersecurity; and DOD's nascent understanding of how to develop more secure weapon systems. DOD weapon systems are more software dependent and more networked than ever before (see figure).

Embedded Software and Information Technology Systems Are Pervasive in Weapon Systems (Represented via Fictitious Weapon System for Classification Reasons)


Targeting systems
Industrial control systems
Identify friend or foe systems
Database
Microelectronics throughout
Flight software system
Controller Area Network bus
Communications systems

Source: GAO analysis of Department of Defense information. | GAO-19-128

Automation and connectivity are fundamental enablers of DOD's modern military capabilities. However, they make weapon systems more vulnerable to cyber attacks. Although GAO and others have warned of cyber risks for decades, until recently, DOD did not prioritize weapon systems cybersecurity. Finally, DOD is still determining how best to address weapon systems cybersecurity.

In operational testing, DOD routinely found mission-critical cyber vulnerabilities in systems that were under development, yet program officials GAO met with believed their systems were secure and discounted some test results as unrealistic. Using relatively simple tools and techniques, testers were able to take control of systems and largely operate undetected, due in part to basic issues such as poor password management and unencrypted communications. In addition, vulnerabilities that DOD is aware of likely represent a fraction of total vulnerabilities due to testing limitations. For example, not all programs have been tested and tests do not reflect the full range of threats.

DOD has recently taken several steps to improve weapon systems cybersecurity, including issuing and revising policies and guidance to better incorporate cybersecurity considerations. DOD, as directed by Congress, has also begun initiatives to better understand and address cyber vulnerabilities. However, DOD faces barriers that could limit the effectiveness of these steps, such as cybersecurity workforce challenges and difficulties sharing information and lessons about vulnerabilities. To address these challenges and improve the state of weapon systems cybersecurity, it is essential that DOD sustain its momentum in developing and implementing key initiatives. GAO plans to continue evaluating key aspects of DOD's weapon systems cybersecurity efforts.