GAO Highlights

Highlights of GAO-22-104195, a report to congressional addressees

September 2022

NUCLEAR WEAPONS CYBERSECURITY:

NNSA Should Fully Implement Foundational Cybersecurity Risk Management Practices

Why GAO Did This Study

NNSA and its site contractors integrate information systems into nuclear weapons, automate manufacturing equipment, and rely on computer modeling to design weapons. However, cyber systems are targets of malicious actors. To protect against such threats, federal law and policies require that NNSA establish a program to manage cybersecurity risk, which includes the implementation of six foundational practices. NNSA contractors are required to oversee subcontractors' cybersecurity.

The Senate committee report accompanying the National Defense Authorization Act for Fiscal Year 2020 included a provision for GAO to review NNSA's cybersecurity practices and policies, and GAO was also asked to perform similar work. GAO's report examines the extent to which (1) NNSA and its seven site contractors implemented foundational cybersecurity risk management practices and (2) contractors oversee subcontractor cybersecurity.

GAO reviewed NNSA and contractor documents, compared NNSA's efforts with federal and agency requirements for risk management practices, and interviewed NNSA officials and contractor representatives.

What GAO Recommends

GAO is making nine recommendations to NNSA, including that it fully implement an IT continuous monitoring strategy; determine needed resources for operational technology efforts; create a nuclear weapons risk strategy; and enhance monitoring of subcontractor cybersecurity. NNSA agreed with GAO's recommendations.

View GAO-22-104195. For more information, contact Allison B. Bawden at (202) 512-3841 or bawdena@gao.gov or David B. Hinchman at 214-777-5719 or hinchmand@gao.gov.

What GAO Found

The National Nuclear Security Administration (NNSA) and its contractors have not fully implemented six foundational cybersecurity risk practices in its traditional IT environment. NNSA also has not fully implemented these practices in its operational technology and nuclear weapons IT environments.

Organization-wide Foundational Practices to Manage Cybersecurity Risk	
Practice 1	Identify and assign cybersecurity roles and responsibilities for risk management.
Practice 2	Establish and maintain a cybersecurity risk management strategy for the organization.
Practice 3	Document and maintain policies and plans for the cybersecurity program.
Practice 4	Assess and update organization-wide cybersecurity risks.
Practice 5	Designate controls that are available for information systems or programs to inherit.
Practice 6	Develop and maintain a strategy to monitor risks continuously across the organization.

Source: GAO analysis based on Office of Management and Budget, National Institute of Standards and Technology, and Committee on National Security Systems guidance. | GAO-22-104195

The **traditional IT environment** includes computer systems used for weapons design. NNSA fully implemented four of six practices and partially implemented two. NNSA contractors had fully implemented three of six practices and did not fully implement three. For example, both NNSA and its contractors had not fully implemented a continuous monitoring strategy because their strategy documents were missing key recommended elements. Without such elements, NNSA and its contractors lack a full understanding of their cybersecurity posture and are limited in their ability to effectively respond to emerging cyber threats.

The **operational technology environment** includes manufacturing equipment and building control systems with embedded software to monitor physical devices or processes. NNSA has not yet fully implemented any foundational risk management practices in this environment, and it is still developing specific guidance for contractors. This is partially because NNSA has not yet determined the resources it needs to implement practices and develop guidance.

The **nuclear weapons IT environment** includes IT in or in contact with weapons. NNSA has implemented or taken action consistent with implementing most of the practices in this environment and is developing specific guidance for contractors. However, NNSA has not developed a cyber risk management strategy to address nuclear weapons IT-specific threats. The absence of such a strategy likely constrains NNSA's awareness of and responses to such threats.

NNSA's cybersecurity directive requires contractors to oversee their subcontractors' cybersecurity measures, but contractors' efforts to provide such oversight are mixed, and three of seven contractors do not believe it is a contractual responsibility. An NNSA official proposed adding an evaluation of such oversight to its annual contractor performance evaluation process, but NNSA could not provide evidence that it had done so. These oversight gaps, at both the contractor and NNSA level, leave NNSA with little assurance that sensitive information held by subcontractors is effectively protected.