



September 2022

NUCLEAR WEAPONS CYBERSECURITY

NNSA Should Fully Implement Foundational Cybersecurity Risk Management Practices

Accessible Version

GAO Highlights

Highlights of [GAO-22-104195](#), a report to congressional addressees

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.

September 2022

NUCLEAR WEAPONS CYBERSECURITY:

NNSA Should Fully Implement Foundational Cybersecurity Risk Management Practices

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

Category	Category description
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.

Contents

GAO Highlights	2
Why GAO Did This Study	2
What GAO Recommends	2
What GAO Found	2
Letter	1
Background	5
NNSA Implemented Foundational Cybersecurity Risk Management Practices More Often in the Traditional IT Environment than in Other Environments	18
Contractor-Required Monitoring of Subcontractor Cybersecurity Is Inconsistent	40
Conclusions	44
Recommendations	45
Agency Comments and Our Evaluation	46

Appendix I: Objectives, Scope, and Methodology	50
Appendix II: Details on NNSA's Implementation of Six Foundational Cybersecurity Risk Management Practices	55
Appendix III: Details on NNSA Contractors' Identification and Assignment of Risk Management Roles and Responsibilities	58
Appendix IV: Details on NNSA Contractors' Establishment and Maintenance of Cybersecurity Risk Management Strategies	61
Appendix V: Details on NNSA Contractors' Documentation and Maintenance of Cybersecurity Program Policies	65
Appendix VI: Details on NNSA Contractors' Assessment and Update of Organizational Cybersecurity Risks	67
Appendix VII: Details on NNSA Contractors' Designation of Controls Available for Inheritance	70
Appendix VIII: Details on NNSA Contractors' Development and Maintenance of Continuous Monitoring Strategies	72
Appendix IX: Comments from the National Nuclear Security Administration	76
Accessible Text for Appendix IX: Comments from the National Nuclear Security Administration	81
Appendix X: GAO Contacts and Staff Acknowledgments	85

Tables

Table 1: Foundational Cybersecurity Risk Management Practices for Establishing Organization-wide Cybersecurity Risk Management Programs	16
Table 2: Foundational Cybersecurity Risk Management Practices for Establishing Organization-wide Cybersecurity Risk Management Programs	51
Table 3: Extent to Which the National Nuclear Security Administration (NNSA) Implemented Six Foundational Cybersecurity Risk Management Practices	55
Table 4: Extent to Which the National Nuclear Security Administration's (NNSA) Management and Operating (M&O) Contractors Identified and Assigned Cybersecurity Risk Management Roles and Responsibilities	58
Table 5: Extent to Which the National Nuclear Security Administration's (NNSA) Management and Operating (M&O) Contractors Established and Maintained Cybersecurity Risk Management Strategies	62

Table 6: Extent to Which the National Nuclear Security Administration's (NNSA) Management and Operating (M&O) Contractors Documented and Maintained Cybersecurity Program Policies and Plans	65
Table 7: Extent to Which the National Nuclear Security Administration's (NNSA) Management and Operating (M&O) Contractors Assessed and Updated Cybersecurity Risks ⁶⁷	
Table 8: Extent to Which the National Nuclear Security Administration's (NNSA) Management and Operating (M&O) Contractors Designated Controls Available for Inheritance by Information Systems or Programs	70
Table 9: Extent to Which the National Nuclear Security Administration's (NNSA) Management and Operating (M&O) Contractors Developed and Maintained Cybersecurity Continuous Monitoring Strategies	73

Figures

Figure 1: Division of Primary Responsibility for the National Nuclear Security Administration's Three Digital Environments	7
Figure 2: National Nuclear Security Administration (NNSA) Sites and Management and Operating Contractors	8
Figure 3: National Nuclear Security Administration (NNSA) and Management and Operating (M&O) Contractors' Implementation of Foundational Cybersecurity Risk Management Practices in the Traditional Information Technology Environment, as of May 2022	20
Accessible Data for Figure 3: National Nuclear Security Administration (NNSA) and Management and Operating (M&O) Contractors' Implementation of Foundational Cybersecurity Risk Management Practices in the Traditional Information Technology Environment, as of May 2022	20

Abbreviations

CMMC	Cybersecurity Maturity Model Certification
CNSS	Committee on National Security Systems
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
FISMA	Federal Information Security Modernization Act
M&O	management and operating
NEA	Nuclear Enterprise Assurance
NNSA	National Nuclear Security Administration
NIST	National Institute of Standards and Technology
NWDA	Nuclear Weapon Digital Assurance
NW-IT	nuclear weapons information technology
OMB	Office of Management and Budget
OT	operational technology
OTA	Operational Technology Assurance
SD	supplemental directive
SP	special publication

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



September 22, 2022

Congressional Addressees

Current U.S. nuclear weapons were developed during the Cold War, when computer capabilities were in their infancy and little consideration was given to cyber vulnerabilities. Weapons currently in the U.S. nuclear stockpile contain relatively little digital technology.

Over the coming 2 decades, however, the National Nuclear Security Administration (NNSA)—a separately organized agency within the Department of Energy (DOE)—will continue to maintain and modernize the stockpile.¹ As it does so, NNSA plans to increasingly integrate digital systems into nuclear weapons, automate manufacturing processes and equipment, and rely on advanced computer processing capabilities to assess weapons and predict performance. Digital systems such as these can be hacked, corrupted, or subverted by malicious actors. They also can be subject to equipment failures, software coding errors, or the accidental actions of employees.

The Office of Management and Budget (OMB)—with support from the Department of Homeland Security (DHS)—oversees federal cybersecurity generally,² and the Office of the National Cybersecurity Director, in partnership with OMB, supports departments and agencies as they plan and budget for the future of their cyber resources.³ The interagency Committee on National Security Systems (CNSS) also coordinates guidance relating specifically to the cybersecurity of national security

¹In addition, NNSA's other missions include defense nuclear nonproliferation and nuclear naval propulsion.

²Per the Federal Information Security Modernization Act of 2014 (FISMA) (Pub. L. No. 113-283, 128 Stat. 3073), DHS is responsible for certain operational aspects of agencies' information security policies and practices, including assisting OMB in fulfilling its FISMA authorities, issuing binding operational directives, monitoring agencies' security policies and practices, and assisting them with implementation. DHS's Cybersecurity and Infrastructure Security Agency is to work with each federal civilian department and agency to promote the adoption of common policies and best practices that are risk based and able to effectively respond to the pace of ever-changing threats.

³Section 1752 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1752, 134 Stat. 3388, 4144 established, within the Executive Office of the President, the Office of the National Cyber Director.

systems.⁴ In addition, the National Institute of Standards and Technology (NIST) develops specific cybersecurity standards and guidelines for federal agencies. NIST has established a risk management framework to provide a consistent and repeatable process for agencies to follow in managing their cybersecurity risk management programs and responding to cybersecurity risks. On the basis of documents from OMB, CNSS, and NIST, we selected six practices to prepare organizations to execute a risk management framework for cybersecurity that, for the purpose of our review, we refer to as “foundational risk management practices.”

NNSA relies on management and operating (M&O) contractors to execute the agency’s mission to maintain and modernize the stockpile at the eight laboratory and production sites.⁵ M&O contractors, in turn, rely on subcontractors to provide various services, equipment, and components. NNSA’s M&O contractors are required to follow DOE and NNSA cybersecurity requirements, which overlay and expound upon the government-wide foundational risk management practices we identified, and to ensure that the thousands of subcontractors they rely on also employ cybersecurity measures.

The classified annex to Senate Report 116-48 accompanying the National Defense Authorization Act for Fiscal Year 2020 includes a provision for us to review NNSA’s practices and policies for the cybersecurity of nuclear weapons, and we were also asked to perform similar work. This report addresses the extent to which (1) NNSA and its M&O contractors have implemented foundational cybersecurity risk management practices; and

⁴For national security systems, National Security Directive 42 established CNSS, an organization chaired by the Department of Defense, to consider technical matters and develop operating policies, procedures, guidelines, instructions, and standards for national security systems. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (July 5, 1990). Under FISMA, a “national security system” includes, for example, an information system used by an agency or contractor for purposes relating to intelligence, command and control of military forces, or equipment integral to a weapon or weapons system. 44 U.S.C. § 3552(6).

⁵NNSA’s eight sites are the national laboratories—Lawrence Livermore National Laboratory (Lawrence Livermore) in California, Los Alamos National Laboratory (Los Alamos) in New Mexico, Sandia National Laboratory (Sandia) in New Mexico and California—and the production sites—Y-12 National Security Complex (Y-12) in Tennessee, the Pantex Plant in Texas, the Kansas City National Security Campus (Kansas City) in Missouri, the Nevada National Security Site (Nevada) in Nevada, and NNSA operations at the Savannah River Site (Savannah River) in South Carolina. NNSA operations at the Savannah River Site in South Carolina are managed by contractors under the DOE’s Office of Environmental Management.

(2) M&O contractors oversee subcontractor cybersecurity, and NNSA efforts to enhance such oversight.

To address the extent to which NNSA and its M&O contractors have implemented foundational risk management practices, we selected six foundational cybersecurity risk management practices from federal cybersecurity policy and guidance.⁶ We also identified DOE orders and NNSA supplemental directives that include requirements that overlay or expound upon the foundational cybersecurity practices.⁷ We collected and reviewed cybersecurity and risk management documentation from NNSA and the seven contractors that manage and operate its eight sites, such as organization and site-level cybersecurity program policies and plans, risk management and continuous monitoring strategies, and risk assessment reports. We assessed the extent to which documentation demonstrated that NNSA addressed the six foundational cybersecurity risk management practices in the three digital environments that NNSA uses to frame its cybersecurity risks. We limited our assessment of contractor implementation of the foundational risk management practices to one environment because NNSA was developing, but did not have, guidance for contractors in two environments. We scored the

⁶Office of Management and Budget, *Managing Information as a Strategic Resource*, OMB Circular A-130 (Washington, D.C.: July 27, 2016); National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy*, NIST Special Publication (SP) 800-37, Revision 2 (Gaithersburg, Md.: December 2018); Committee on National Security Systems, *Cybersecurity Risk Management*, CNSS Policy 22 (Fort Meade, Md.: August 2016); and Committee on National Security Systems, *Security Categorization and Control Selection for National Security Systems*, CNSS Instruction 1253 (Fort Meade, Md.: March 2014). The practices we selected are expected of all federal agencies, and similar practices have been assessed in our prior work. See GAO, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, [GAO-19-384](#) (Washington, D.C.: July 25, 2019).

⁷Department of Energy, *Department of Energy Cybersecurity Program*, Order 205.1C (Washington, D.C.: Feb. 3, 2022); Department of Energy, *Security and Use Control of Nuclear Explosives and Nuclear Weapons*, Order 452.4C (Washington, D.C.: Aug. 28, 2015); National Nuclear Security Administration, *Baseline Cybersecurity Program*, Supplemental Directive (SD) 205.1 (Washington, D.C.: July 6, 2017); and National Nuclear Security Administration, *Directives Management*, SD 251.1B (Washington, D.C.: Oct. 26, 2020).

documentation against the six practices, using a five-tiered rating scale.⁸ We also interviewed DOE and NNSA officials responsible for cybersecurity or contractor oversight and conducted semistructured interviews with federal officials and contractor representatives from each of NNSA's eight laboratory and production sites regarding their perspectives on implementing the foundational cybersecurity practices.

To examine the extent to which M&O contractors oversee subcontractor cybersecurity and NNSA efforts to enhance such oversight, we first reviewed contractor cybersecurity requirements specified in the relevant DOE order and NNSA directive. We also reviewed each of the seven M&O contracts and draft versions of proposed revisions to the supplemental directive. On the basis of this documentation, we identified current and potential requirements for contractors to ensure that subcontractors employ cybersecurity measures. We interviewed DOE and NNSA officials regarding NNSA's oversight of contractors and potential efforts to enhance cybersecurity oversight. We also conducted semistructured interviews with M&O contractor representatives from the sites to determine the extent to which cybersecurity contract requirements were clearly understood by M&O contractors and were being applied to subcontractors. More details on our objectives, scope, and methodology are provided in appendix I.

We conducted this performance audit from March 2020 to September 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

⁸We based the rating scale using five implementation tiers: (1) fully implemented—NNSA and its contractors addressed all of the practice's elements; (2) substantially implemented—NNSA and its contractors more than partially addressed the practice's elements, but not all; (3) partially implemented—NNSA and its contractors addressed about half of the practice's elements; (4) minimally implemented—NNSA and its contractors addressed some, but a minority, of the practice's elements, and (5) not implemented—NNSA and its contractors did not address any of the practice's elements.

Background

NNSA's Digital Environments

NNSA operates in three broad digital environments—information technology (IT), operational technology (OT), and nuclear weapons IT (NW-IT).

- **Traditional IT** is any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, according to OMB guidance.⁹ According to NNSA officials, traditional IT systems within NNSA can include all types of computing platforms, such as general-purpose computing systems, cloud systems,¹⁰ supercomputers, and other information systems that support weapon development activities such as research, system design, component design, modeling, simulation, and interfaces between NNSA's sites.¹¹
- **OT** is any hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events, according to DOE Order 205.1C, *Department of Energy Cybersecurity Program*. In general, OT includes industrial control systems and supervisory control and data acquisition systems used in critical infrastructures such as water, oil and gas pipelines, energy, and utilities. These systems can include electrical, mechanical, hydraulic, and pneumatic components that support

⁹Office of Management and Budget, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

¹⁰NIST defines cloud computing as a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned and released. This approach offers federal agencies a means to buy services more quickly and possibly at a lower cost than building, operating, and maintaining these computing resources themselves.

¹¹NNSA refers to such systems as "enterprise" IT systems. To avoid confusions with the nuclear security enterprise, however, we refer to such systems as "traditional" IT systems in this report.

manufacturing and transportation. In the context of the U.S. nuclear security enterprise, OT systems are the processes, equipment, materials, and products employed in the production of nuclear weapons. This includes facilities across the entire nuclear security enterprise, a wide array of production equipment, and thousands of different tester systems.¹²

- **NW-IT** refers to IT contained within a warhead or bomb to include all configurations that support activities such as stockpile surveillance; flight testing; testing for compatibility with Department of Defense (DOD) systems; and training, among other activities.¹³ The broader weapon system, such as DOD-supplied delivery system components, subsystems, and systems, is not considered NW-IT.

NNSA's Organization and Contractor Oversight Responsibilities

To support its mission of maintaining a safe and reliable nuclear weapons stockpile, NNSA is organized into offices that oversee information management and cybersecurity, stockpile sustainment and modernization programs, and acquisitions and contract oversight.¹⁴ Specifically, the Office of Information Management (Information Management), which includes the Associate Administrator for Information Management and Chief Information Officer, is broadly responsible for implementing cybersecurity within NNSA. This office retains oversight responsibility for IT and OT systems but in March 2019 delegated authority for NW-IT to NNSA's Office of Defense Programs (Defense Programs), which

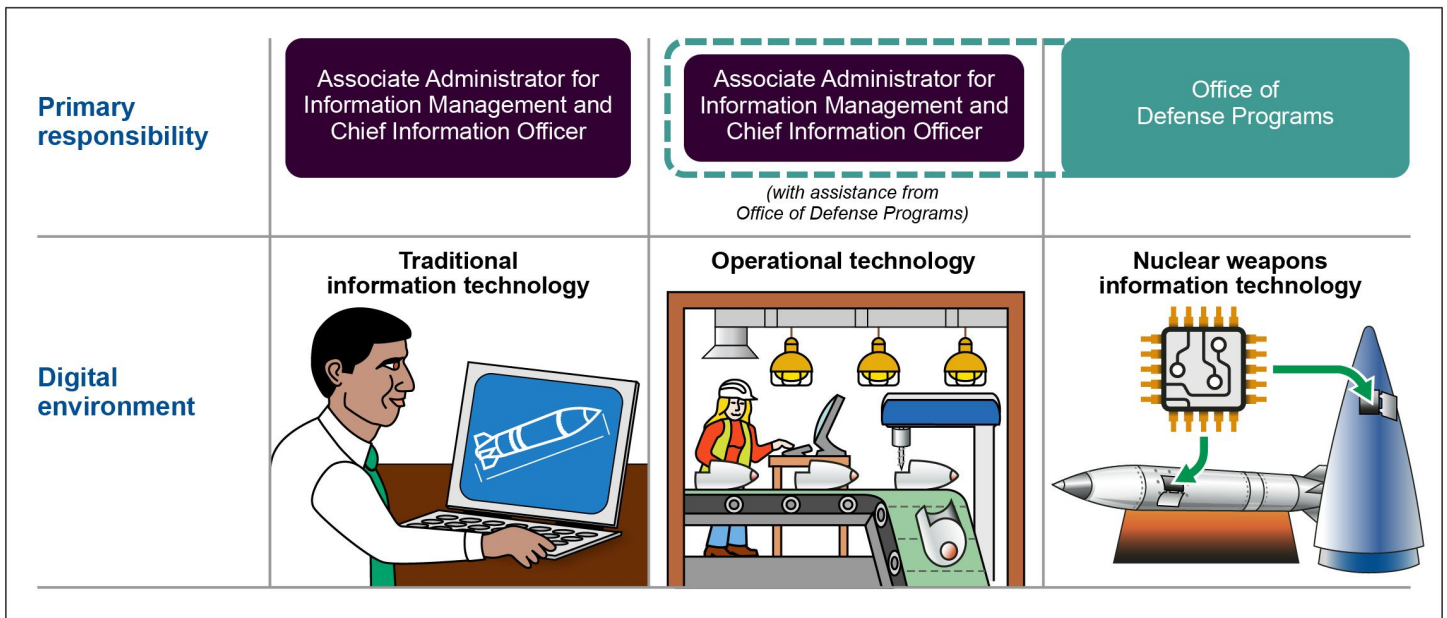
¹²Data from test equipment provide evidence for process qualification, weapon certification, reliability, surety, product acceptance, and stockpile evaluation and are used to evaluate performance at all levels of assembly. Many items of test equipment are one-of-a-kind, custom-designed, and custom-built apparatuses that test classified assemblies.

¹³All nuclear weapons in the U.S. stockpile are designated as either a warhead or a bomb. Modern nuclear weapons consist of three sets of components—a primary, a secondary, and a set of nonnuclear components—enclosed in a bomb or warhead/missile case. Warheads and bombs are weapons that have certain engineering requirements because they must interface with a launch or delivery system, such as with an intercontinental ballistic missile.

¹⁴"Stockpile sustainment" refers to the activities for maintaining the day-to-day health of the nuclear weapons stockpile. These activities include surveillance, annual assessments, and routine maintenance. Weapons that remain in the stockpile eventually undergo modernization programs—such as life extension programs or modification programs—to address any anomalies and to meet updated safety and security standards. Stockpile modernization may also refer to future weapons programs under consideration.

oversees stockpile sustainment and weapons development. An October 2019 Defense Programs memorandum further directed Defense Programs to support Information Management in the risk management of OT systems (see fig.1).

Figure 1: Division of Primary Responsibility for the National Nuclear Security Administration’s Three Digital Environments

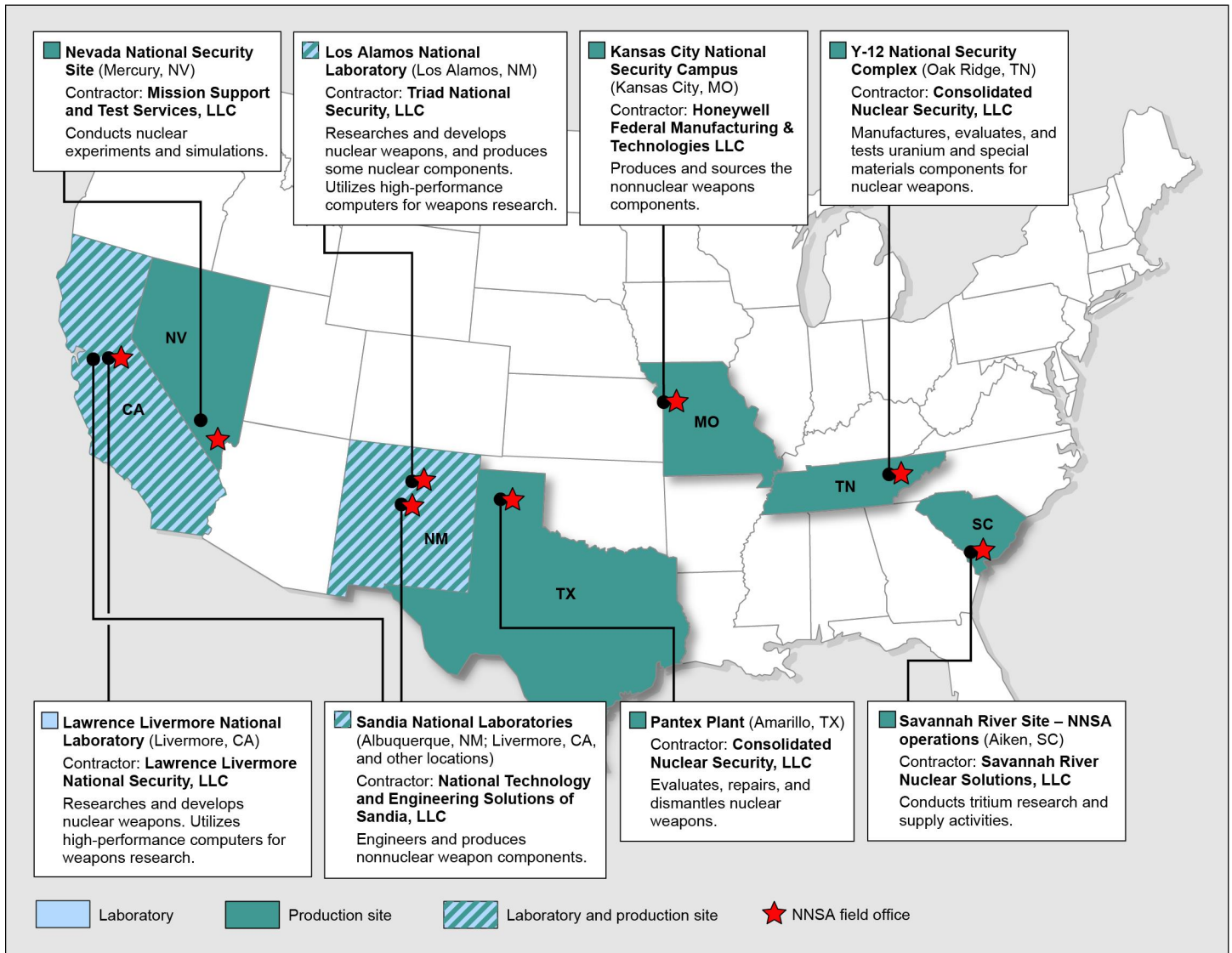


Source: GAO analysis of National Nuclear Security Administration information. | GAO-22-104195

The eight federally owned, contractor-operated laboratory and production sites across the country that execute NNSA’s missions operate in combinations of the three digital environments. The nature of NNSA’s relationship with M&O contractors in managing and operating government-owned or government-controlled facilities is recognized in procurement rules. The Federal Acquisition Regulation—which describes uniform policies and procedures for acquisition by executive agencies—describes this relationship as one where the work conducted by the contractor is of a long-term or continuing nature, involving high levels of expertise and continuity of operations and personnel.

NNSA is responsible for managing and overseeing the mission-related and mission-support activities undertaken by its contractors at the laboratories and production sites known collectively as the nuclear security enterprise, as shown in figure 2.

Figure 2: National Nuclear Security Administration (NNSA) Sites and Management and Operating Contractors



Sources: GAO presentation of NNSA information; Map Resources (map). | GAO-22-104195

Note: The Pantex Plant and Y-12 National Security Complex are separate sites managed and operated by a common contractor under a single federal contract. The two sites are overseen by a single field office with locations at both sites. NNSA operations at the Savannah River Site in South Carolina are managed by contractors under the Department of Energy’s Office of Environmental Management.

NNSA’s Office of Acquisition and Project Management focuses on contract oversight and provides direct lines of authority and accountability

for federal and contractor personnel, among other things.¹⁵ Its objective is to ensure that NNSA implements DOE's acquisition and project management policies and regulations, as well as NNSA's own supplemental directives and procedures. NNSA's local offices, also known as field offices, oversee contractors and seek to ensure that contract awards are appropriate, that all requirements of law and regulation are met prior to executing a contract action, and that both NNSA and the contractor comply with the terms of the prime contract.

NNSA develops Performance Evaluation and Measurement Plans at the beginning of each fiscal year to establish expectations for contractor performance and to describe how the site contracting officers will evaluate the contractors' performance against those expectations. At the end of the review period, typically the end of the fiscal year, NNSA documents the contractor's performance rating and, in some cases, the fees and other incentives that will be awarded to the contractor in a Performance Evaluation Report.¹⁶

In the execution of their contract, contractors may hire and manage subcontractors. M&O contractors are responsible for subcontract

¹⁵According to NNSA officials in May 2022, NNSA is planning a reorganization of the acquisition and project management functions for later in fiscal year 2022. Officials noted that the contract oversight function of this office is likely to transition to another office within NNSA.

¹⁶Since 1990, DOE's management of contracts and projects, including those executed by NNSA, has been on our list of areas at high risk for fraud, waste, abuse, and mismanagement. See GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, [GAO-21-119SP](#) (Washington, D.C.: Mar. 2, 2021). In 2019, we reported that in fiscal years 2006 through 2016, six offices within DOE generally used one of three different approaches to evaluate M&O contractor performance. Although these approaches varied in the performance criteria and methodologies used for determining contractor ratings and incentives, all the offices annually set expectations for contractors and assessed performance. GAO, *Department of Energy: Performance Evaluations Could Better Assess Management and Operating Contractor Costs*, [GAO-19-5](#) (Washington, D.C.: Feb. 26, 2019).

oversight.¹⁷ A contractor may enter into a subcontract to obtain access to a specific set of skills or services that it may not possess, such as construction expertise, equipment services, or technology support. Subcontractors may handle unclassified and unclassified but sensitive information, have access to classified information, or provide capabilities that will be used by the contractor to execute NNSA's mission.¹⁸

For example, in the IT environment, subcontractors may provide IT assets—including computer systems, servers, and software—or assist in the rollout of the next generation of high-performance computers. In the OT environment, subcontractors may provide equipment used to manufacture components used within a weapon. In the NW-IT environment, subcontractors may directly provide components incorporated into a weapon. Contractors are required by their contracts to comply with DOE and NNSA cybersecurity requirements; these requirements include provisions requiring the contractor to oversee the cybersecurity measures that subcontractors implement.

¹⁷DOE and NNSA oversee contractors' subcontract management in three broad categories: (1) reviewing subcontract costs, including conducting certain subcontract audits, to ensure that subcontract costs are appropriately charged to prime contracts; (2) reviewing and approving contractor business systems, including contractor accounting and purchasing systems, to ensure validity of data and sufficiency of subcontract oversight policies and procedures; and (3) performing subcontract consent reviews prior to certain subcontract awards to consider whether the contractor is complying with contract provisions and assuring against conflicts of interest, such as close working relationships or ownership affiliations between the contractor and subcontractor, which may preclude free competition or result in higher prices. See GAO, *Department of Energy Contracting: Actions Needed to Strengthen Subcontract Oversight*, [GAO-19-107](#) (Washington, D.C.: Mar. 12, 2019).

¹⁸We have previously reported that DOE and NNSA do not explicitly evaluate their contractors' management of subcontracts as part of the annual performance evaluation process because DOE officials said that the contractor is responsible for completing the scope of work in the contract, regardless of whether it was performed by the contractor or a subcontractor. We recommended that DOE include explicit performance criteria that assess the contractors' management of subcontractors as part of its contractor expectations. DOE partially concurred with this recommendation but, as of April 2022, held that sufficient guidance existed for contracting officers to make informed decisions on whether to include contractor management of subcontractors as part of the annual assessment process. See [GAO-19-107](#).

Cybersecurity Threats to Federal Agencies and the Private Sector

Federal agencies, such as NNSA, and private sector companies are increasingly dependent on IT and OT systems to execute mission and business objectives. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions without these information assets. In addition, many of these systems contain vast amounts of sensitive or classified data, making it imperative to protect them.

Safeguarding federal computer systems has been a long-standing concern and, underscoring the importance of this issue, we have included cybersecurity on GAO's High Risk List since 1997.¹⁹ Recent, increasingly sophisticated cyber incidents at federal agencies and in the private sector demonstrate the damage that advanced threats can cause and reinforce the importance of effectively protecting systems that process federal information and data. For example, we reported on two recent incidents of significant concern:²⁰

- One of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector involved SolarWinds—a Texas-based network management software company.²¹
- Another incident involving Microsoft Exchange Server vulnerabilities had the potential to affect email servers across the federal

¹⁹[GAO-21-119SP](#).

²⁰See GAO, *Cybersecurity: Federal Responses to SolarWinds and Microsoft Exchange Incidents*, [GAO-22-104746](#) (Washington, D.C.: Jan. 13, 2022).

²¹Beginning as early as January 2019, a threat actor breached the computing networks at SolarWinds. The federal government later confirmed the threat actor to be the Russian Foreign Intelligence Service. Since the company's software, SolarWinds Orion, was widely used in the federal government to monitor network activity and manage network devices on federal systems, this incident allowed the threat actor to compromise several federal agencies' networks that used the software.

government and provide malicious threat actors with unauthorized remote access.²²

According to the Cybersecurity and Infrastructure Security Agency, the potential exploitation from both incidents posed an unacceptable risk to federal civilian executive branch agencies because of the likelihood of vulnerabilities being exploited and the prevalence of affected software.²³ A May 2021 ransomware attack on the Colonial Pipeline oil company also critically impacted its business systems, and the company proactively disconnected certain industrial control systems to prevent further compromise. The attack resulted in a temporary shortage of gasoline throughout much of the southeastern United States.²⁴ In addition, a May 2021 ransomware attack on Sol Oriens, LLC—a technology research and development subcontractor to an NNSA contractor—led to the unauthorized disclosure and public posting of invoices for NNSA contracts and descriptions of research and development projects managed by defense and energy contractors, according to media reports.²⁵

²²In March 2021, Microsoft reported the exploitation or misuse of vulnerabilities used to gain access to several versions of Microsoft Exchange Server. This included versions that federal agencies hosted and used on their premises. The vulnerabilities initially allowed threat actors to make authenticated connections to Microsoft Exchange Servers from unauthorized external sources. Once the threat actor made a connection, the actor then could leverage other vulnerabilities to escalate account privileges and install web shells (i.e., a malicious script or program that runs on an operating system) that enabled the actor to remotely access a Microsoft Exchange Server.

²³Cybersecurity and Infrastructure Security Agency, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, Emergency Directive 21-02 (Mar. 3, 2021). This directive required federal civilian departments and agencies running Microsoft Exchange on-premises products to update or disconnect the products from their networks until updated with the Microsoft patch.

²⁴GAO, *Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness*. <https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic>.

²⁵According to media reports, Sol Oriens said that it has no current indication that this incident involved classified or critical security-related information.

FISMA, OMB Policy, and a Recent Executive Order Establish Requirements for Protecting Federal Systems and Managing Cybersecurity Risks

Several federal laws, executive orders, and policies establish cybersecurity requirements for protecting federal systems and managing cyber risks. These include the following:

- **The Federal Information Security Modernization Act of 2014 (FISMA).** In 2014, Congress passed FISMA, which requires agencies such as DOE and NNSA to develop, document, and implement a program to provide security for the information and information systems that support the operations and assets of the agency.²⁶
- **OMB Circular A-130, Managing Information as a Strategic Resource.** In July 2016, OMB updated this circular to establish minimum requirements for federal cybersecurity programs, assign federal agency responsibilities for the security of information and information systems, and link agency cybersecurity programs and management control systems established in accordance with OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.²⁷
- **Executive Order 14028, Improving the Nation's Cybersecurity.** In May 2021, the President issued an executive order that directs the federal government to bring to bear the full scope of its authorities and resources to protect and secure its computer systems.²⁸ The order noted that protection and security must include systems that process data—IT systems—and those that run the vital machinery that ensures our safety—OT systems.

²⁶The 2014 revision of FISMA largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

²⁷OMB Circular A-130.

²⁸The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

Guidance and Advisories Establish Further Cybersecurity Guidelines and Resources for Federal Agencies

Guidance from NIST and CNSS establish guidelines for federal agencies to apply a cybersecurity risk management framework to their mission objectives, business processes, and activities. In addition, the National Security Agency and DOD have, or are creating, additional resources for securing federal data and networks. Specifically,

- **NIST guidance.** NIST is responsible for developing standards for categorizing information and information systems, security requirements for information and systems, and guidelines for detection and handling of security incidents. Specific examples of guidance include the following:
 - NIST Special Publication (SP) 800-37, Revision 2, which establishes a risk management framework to provide a consistent and repeatable process for agencies to follow in managing their cybersecurity risk management programs and responding to cybersecurity risks.²⁹
 - NIST SP 800-53, Revision 5, which provides guidance to agencies on the selection and implementation of information security and privacy controls for systems.³⁰
 - NIST SP 800-171, Revision 2, which provides recommended security requirements for protecting the confidentiality of controlled unclassified information that resides in nonfederal systems and organizations.³¹
- **CNSS guidance.** CNSS—an interagency organization chaired by DOD—coordinates guidance and issues policy directives and instructions relating specifically to the cybersecurity of national security systems. CNSS Policy 22 provides guidance to agencies on establishing an integrated, organization-wide cybersecurity risk

²⁹NIST SP 800-37.

³⁰National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, Revision 5 (Gaithersburg, MD: September 2020).

³¹National Institute of Standards and Technology, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, SP 800-171, Revision 2 (Gaithersburg, Md.: February 2020).

management program. CNSS Instruction 1253 provides all federal government departments, agencies, bureaus, and offices with guidance on the first steps of the risk management framework.

- **National Security Agency advisory.** In April 2021, the National Security Agency issued a Cybersecurity Advisory stating that the United States needs to significantly shift how OT systems are viewed, evaluated, and secured to prevent malicious cyber actors from executing successful, and potentially damaging, cyber effects.³² This advisory included an evaluation methodology and a basic cybersecurity improvement approach for organizations faced with limited resources.
- **DOD guidance.** In 2019, DOD started creating the Cybersecurity Maturity Model Certification (CMMC) framework as a response to a call for a unifying cybersecurity standard for its defense contractors—known as its defense industrial base.³³ As we have reported, CMMC is designed to provide increased assurance that a contractor can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multitier supply chain.³⁴ CMMC is limited to systems handling controlled unclassified information—unclassified information throughout the executive branch that requires safeguarding and dissemination controls in accordance with laws, regulations, and government-wide policies. DOD modified this framework in 2021 to condense its original five levels into three, with required implementation dependent on the sensitivity of the information to be protected.³⁵

³²National Security Agency, *Stop Malicious Cyber Activity Against Connected Operational Technology* (Fort Meade, Md.: April 2021).

³³The defense industrial base comprises all the companies that enable research and development, as well as design, production, delivery, and maintenance of military weapon systems, components, or parts to meet U.S. military requirements.

³⁴GAO, *Defense Contractor Cybersecurity: Stakeholder Communication and Performance Goals Could Improve Certification Framework*, [GAO-22-104679](#) (Washington, D.C.: Dec. 8, 2021).

³⁵To achieve the lowest level—level 1 certification—companies will need to submit an annual self-assessment that they are in compliance with basic cybersecurity practices. For level 2, some companies that process, transmit, or store controlled unclassified information will be required to pass a third-party assessment to achieve certification based on its implementation of all practices contained in NIST guidance. To achieve the highest level—level 3—companies will need to pass a government-led assessment of its implementation of the practices in NIST guidance.

Federal Policy and Guidance Include Six Foundational Cybersecurity Risk Management Practices

OMB policy and guidance from NIST and CNSS include a number of practices for establishing organization-wide cybersecurity risk management programs.³⁶ To prepare agencies to execute a cybersecurity risk management framework, these documents address common practices that can be distilled into six key practices.³⁷ For the purpose of our review, we refer to these six key practices as foundational practices for establishing an organization-wide cybersecurity risk management program. The six foundational cybersecurity risk management practices are applicable to any of NNSA's digital operating environments and should be tailored based on mission objectives and the risks of that particular digital environment. Practices that provide a foundation for an organization's cybersecurity risk management program are summarized in table 1.

Table 1: Foundational Cybersecurity Risk Management Practices for Establishing Organization-wide Cybersecurity Risk Management Programs

Foundational practices	Foundational practices (description)	Description
Practice 1	Identify and assign cybersecurity risk management roles and responsibilities.	In order to ensure that cybersecurity risks are being addressed across the organization, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 states that organizations should identify and assign individuals or a group to specific roles and responsibilities. ^a The intent of this practice is to provide organization-wide oversight of cybersecurity risk activities and facilitate collaboration among stakeholders and consistent application of the cybersecurity risk management strategy.

³⁶National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST SP 800-39 (Gaithersburg, Md.: March 2011). NIST SP 800-39 defines an organization as an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements) that is charged with carrying out assigned mission/business processes and that uses information systems in support of those processes.

³⁷Federal policy and guidance include OMB Circular A-130, CNSS Policy 22, and NIST SP 800-37.

Foundational practices	Foundational practices (description)	Description
Practice 2	Establish and maintain a cybersecurity risk management strategy for the organization.	According to the Office of Management and Budget (OMB) Circular A-130 and guidance from NIST SP 800-37 and the Committee on National Security Systems (CNSS) Policy 22, organizations should establish and maintain a risk management strategy. NIST SP 800-37 describes nine elements of a risk management strategy. ^b CNSS Instruction 1253 requires organizations to review and update their risk management strategies at least annually. Additionally, according to NIST SP 800-53, organizations should review and update their strategies to address organizational changes. The intent of this practice is to develop a foundation for managing cybersecurity risk and delineate the boundaries for risk-based decisions, which should inform how cybersecurity risk is framed, assessed, responded to, and monitored.
Practice 3	Document and maintain cybersecurity program policies and plans.	According to OMB Circular A-130, agencies must document and maintain organization-wide cybersecurity programs and plans to hold federal personnel and contractors accountable for complying with organizational cybersecurity requirements and policies.
Practice 4	Assess and update organization-wide cybersecurity risks.	According to NIST SP 800-37, organizations should assess organization-wide cybersecurity risk and update results on an ongoing basis. CNSS Policy 22 directs organizations to conduct risk assessments and identify cybersecurity risks from an organization-wide perspective. The intent of this practice is to allow the agency to consider all cyber-related risk derived from the operation and use of its information systems.
Practice 5	Designate controls that are available for information systems or programs to inherit.	According to OMB Circular A-130, NIST SP 800-37, and CNSS Policy 22, organizations should identify, document, and publish controls available for inheritance by information systems or programs. ^c The intent of this practice is to provide cost-effective cybersecurity capabilities that can be inherited by multiple information systems or programs.
Practice 6	Develop and maintain an organization-wide continuous monitoring strategy.	According to OMB Circular A-130, NIST SP 800-37, and CNSS Policy 22, organizations should develop and maintain a continuous monitoring strategy. The circular also requires agencies to update their strategy according to organization-defined frequency. Additionally, NIST guidance describes seven elements of a continuous monitoring strategy. ^d The intent of this practice is to provide for continuous monitoring of an organization's cybersecurity posture and respond to emerging cyber threats in an efficient and cost-effective manner.

Source: GAO analysis based on OMB, CNSS, and NIST guidance. | GAO-22-104195

^aAccording to NIST SP 800-37 Revision 2, key participants in risk management processes include (1) the head of an agency, (2) the authorizing official or authorizing official designated representative, (3) the chief information officer, (4) the senior accountable official for risk management or risk executive function, and (5) the senior agency information security officer.

^bAccording to NIST SP 800-37, Revision 2, a risk management strategy should include several elements. These elements include (1) expressing organizational risk tolerance; (2) guiding and informing risk-based decisions that describe how security risk is framed, assessed, responded to, and monitored; (3) determining risk assessment methodologies; (4) determining risk response strategies; (5) defining a process for consistently evaluating security risks organization-wide; (6) describing considerations for supply chain risk; (7) defining approaches for monitoring risk over time; (8) defining strategic-level decisions and considerations for how senior leaders and executives are to manage cybersecurity risks to organizational operations, organizational assets, individuals, other organizations, and the nation; and (9) including an explicit statement of the threats, assumptions, constraints, priorities, trade-offs, and risk tolerance used for making investment and operational decisions.

^cAccording to NIST SP 800-37, Revision 2, control inheritance is a situation in which a system or application receives protection from controls (or portions of controls) that are developed, implemented, assessed, authorized, and monitored by internal or entities external to the organization other than those responsible for the system or application where it resides.

^dAccording to NIST SP 800-37, Revision 2, a continuous monitoring strategy should include several elements. These elements include (1) considering supply chain risk, (2) addressing monitoring requirements across the organization, (3) identifying the minimum monitoring frequency for implemented security controls across the organization, (4) defining the ongoing control assessment approach, (5) describing how ongoing assessments are to be conducted, (6) defining security reporting requirements and recipients of the reports, and (7) authorizing the strategy for approval by the senior accountable official for risk management or the risk executive (function).

DOE orders and NNSA supplemental directives include cybersecurity requirements that overlay or expound upon OMB policy and CNSS and NIST guidance.³⁸ For example, with respect to practice 2—establish and maintain a cybersecurity risk management strategy for the organization—DOE Order 205.1C and NNSA Supplemental Directive 205.1 require that NNSA document its organization-wide risk management strategy in its cybersecurity program plan. In addition, with respect to practice 3—document and maintain cybersecurity program policies and plans—DOE Order 205.1C requires the cybersecurity program plan to be reviewed and updated annually.

NNSA Implemented Foundational Cybersecurity Risk Management Practices More Often in the Traditional IT Environment than in Other Environments

NNSA and its M&O contractors have fully implemented most of the foundational cybersecurity risk management practices in the traditional IT environment, but NNSA has implemented fewer of these same practices in the OT and NW-IT environments.³⁹ In the traditional IT environment, NNSA has fully implemented four of six foundational risk management practices—such as identifying and assigning cybersecurity risk management roles and responsibilities—while the M&O contractors have fully implemented three of six foundational risk management practices,

³⁸Department orders and agency supplemental directives include DOE Order 205.1C and NNSA SD 205.1.

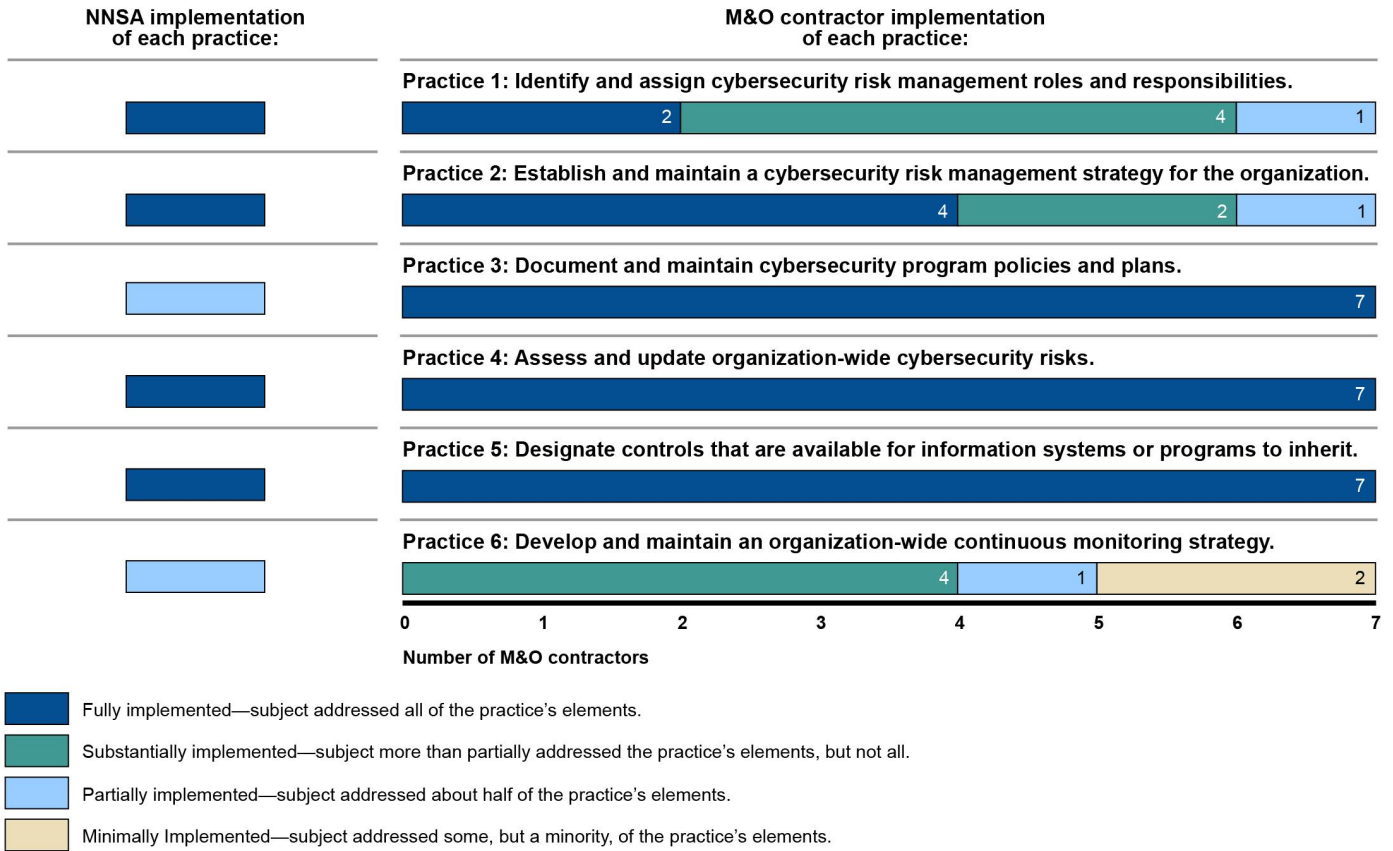
³⁹During our review, NNSA was developing, but did not have, guidance tailored to the OT and NW-IT environments for contractors to implement a cybersecurity risk management framework. Therefore, we focused on NNSA's organization-level efforts and did not assess its contractors' efforts to implement a cybersecurity risk management framework in the OT and NW-IT environments.

including documenting and maintaining cybersecurity program policies and plans. In the OT environment, NNSA has not fully implemented any of the foundational risk management practices, in part because it has not identified the resources necessary to achieve full implementation. Finally, in the NW-IT environment, NNSA has implemented one foundational risk management practice to address NW-IT cybersecurity and is making progress toward implementing most additional practices.

NNSA and Its M&O Contractors Implemented Most of the Foundational Cybersecurity Risk Management Practices in the Traditional IT Environment

In the traditional IT environment, NNSA fully implemented four of the six foundational risk management practices for organization-wide cybersecurity risk management and partially implemented the remaining two. At the site level, the seven M&O contractors that manage and operate NNSA sites fully implemented three of the six foundational risk management practices but did not fully implement the other three practices. Figure 3 summarizes our assessment of the extent to which NNSA and the seven M&O contractors implemented the six foundational risk management practices in the traditional IT environment.

Figure 3: National Nuclear Security Administration (NNSA) and Management and Operating (M&O) Contractors' Implementation of Foundational Cybersecurity Risk Management Practices in the Traditional Information Technology Environment, as of May 2022



Source: GAO analysis of NNSA M&O contractor information. | GAO-22-104195

Accessible Data for Figure 3: National Nuclear Security Administration (NNSA) and Management and Operating (M&O) Contractors' Implementation of Foundational Cybersecurity Risk Management Practices in the Traditional Information Technology Environment, as of May 2022

Number of M&O contractors

Practice 1: Identify and assign cybersecurity risk management roles and responsibilities.

Fully Implemented: 2

Substantially Implemented: 4

Partially Implemented: 1

Practice 2: Establish and maintain a cybersecurity risk management strategy for the organization.

Fully Implemented: 4

Substantially Implemented: 2

Partially Implemented: 1

Practice 3: Document and maintain cybersecurity program policies and plans.

Fully Implemented: 7

Practice 4: Assess and update organization-wide cybersecurity risks.

Fully Implemented: 7

Practice 5: Designate controls that are available for information systems or programs to inherit.

Fully Implemented: 7

Practice 6: Develop and maintain an organization-wide continuous monitoring strategy.

Substantially Implemented: 4

Partially implemented: 1

Minimally Implemented: 2

Fully implemented—subject addressed all of the practice’s elements.

Substantially implemented—subject addressed more than half, but not all, of the practice’s elements.

Partially implemented—subject addressed about half of the practice’s elements.

Minimally Implemented—subject addressed less than half of the practice’s elements.

NNSA implementation of each practice at the organizational level:

- Practice 1 Fully implemented—NNSA addressed all of the practice’s elements
- Practice 2 Fully implemented—NNSA addressed all of the practice’s elements
- Practice 3 Partially implemented—NNSA addressed about half of the practice’s elements

-
- Practice 4 Fully implemented—NNSA addressed all of the practice’s elements
 - Practice 5 Fully implemented—NNSA addressed all of the practice’s elements
 - Practice 6 Partially implemented—NNSA addressed about half of the practice’s elements

NNSA Implementation of Foundational Practices for Traditional IT

As of May 2022, NNSA fully implemented four foundational risk management practices in the traditional IT environment:

- Practice 1: Identify and assign cybersecurity risk management roles and responsibilities.
- Practice 2: Establish and maintain an organization-wide cybersecurity risk management strategy.
- Practice 4: Assess and update organization-wide cybersecurity risks.
- Practice 5: Designate controls that are available for information systems or programs to inherit.

For example, to identify and assign cybersecurity risk management roles and responsibilities, NNSA established a risk executive function managed by the chief information security officer and a risk governance structure through its Enterprise Cybersecurity Advisory Board. To establish and maintain an organization-wide cybersecurity risk management strategy, NNSA established a strategy through its April 2016 Cybersecurity Program Plan, which fully addressed all elements included in NIST guidance. It also performed a review of the strategy to account for organizational changes in October 2021.⁴⁰

To assess and update organization-wide cybersecurity risks, NNSA conducted a risk assessment through its September 2020 *Enterprise*

⁴⁰According to NIST SP 800-37, Revision 2, a risk management strategy should include several elements. These elements include (1) expressing organizational risk tolerance; (2) guiding and informing risk-based decisions that describe how security risk is framed assessed, responded to, and monitored; (3) determining risk assessment methodologies; (4) determining risk response strategies; (5) defining a process for consistently evaluating security risks organization-wide; (6) describing considerations for supply chain risk; (7) defining approaches for monitoring risk over time; (8) defining strategic-level decisions and considerations for how senior leaders and executives are to manage cybersecurity risks to organizational operations, organizational assets, individuals, other organizations, and the nation; and (9) including an explicit statement of the threats, assumptions, constraints, priorities, trade-offs, and risk tolerance used for making investment and operational decisions.

Assessment Report and updated its assessment results through its enterprise risk register (i.e., a management tool—which tracks and manages organizational cybersecurity risks) on a quarterly basis. In addition, to designate controls that are available for information systems or programs to inherit, NNSA identified, documented, and published an organization-wide catalog of security controls—such as incident handling, monitoring, and reporting—through its *Cyber Security Program Plan*.⁴¹

However, NNSA only partially implemented the other two foundational risk management practices in the traditional IT environment. Specifically,

- **Document and maintain cybersecurity program policies and plans (practice 3).** NNSA documented cybersecurity risk-based policies and plans in its July 2017 Supplemental Directive (SD) 205.1, *Baseline Cybersecurity Program*, and April 2016 *Cyber Security Program Plan*, respectively. The organization performed a review and update to its *Cyber Security Program Plan* in October 2021 but, as of May 2022, had not done the same for SD 205.1 within the time frames specified in its directive.

Specifically, NNSA SD 251.1B, *Directives Management*, requires the organization to review directives, such as SD 205.1, every 3 years to confirm relevancy and accuracy, and further requires that documents be consistent with statutes, regulations, and other DOE and NNSA directives.⁴² However, the organization had not completed such a review of this document for nearly 5 years. Furthermore, NNSA had not updated this document to reflect new or revised NIST guidance and other changes required by DOE cybersecurity requirements.

NNSA officials acknowledged that gaps exist in fully implementing this practice. They attributed delays in maintaining its supplemental directive to the organization's lengthy internal review, comment, and approval process for major revisions, in addition to recent administrative changes to key stakeholders. NNSA officials have delayed issuance of the revised directive several times—they first

⁴¹According to NIST, security control inheritance is defined as a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by internal or external entities other than those responsible for the system or application.

⁴²According to NNSA's *Directives Management*, SD 251.1B, supplemental directives establish, communicate, and institutionalize mandatory policies, requirements, responsibilities, and procedures specific to NNSA federal organizations. Supplemental directives can apply to contractors through incorporation into their contracts.

expected to issue it by December 2020, then successively pushed the date to June or July 2021, December 2021, and June 2022. In May 2022, NNSA officials provided to us a draft version of SD 205.1 dated April 2022, but they did not have an estimated completion date for this directive.

While the organization has made progress to incorporate updated guidance in its draft directive, we found that it contained gaps with respect to cybersecurity requirements. Specifically, the draft did not include specific references to two cybersecurity elements that would align it with OMB policy and CNSS guidance. These elements are to review and update risk management and continuous monitoring strategies within prescribed time frames. For instance, the draft version of SD 205.1 that we reviewed did not specify time frames for NNSA and its M&O contractors to perform periodic reviews and updates to these strategies.

Without maintaining cybersecurity program policies and plans, as specified in OMB policy, NNSA's risk-based documents contain gaps—such as missing foundational risk management practice elements—that undermine its efforts to establish clear and up-to-date cybersecurity expectations for its federal employees and contractors.

- **Develop and maintain an organization-wide continuous monitoring strategy (practice 6).** NNSA developed and kept updated an organization-wide continuous monitoring strategy in its April 2021 *Information Systems Continuous Monitoring Plan*, but the strategy did not address all NIST elements.⁴³ For instance, the strategy generally focused on continuous monitoring requirements for individual systems but did not address four of seven NIST elements on organization-wide continuous monitoring. Specifically, the strategy did not address the following elements:
 - considering supply chain risk,

⁴³According to NIST SP 800-37, Revision 2, a continuous monitoring strategy should include several elements. These elements include (1) considering supply chain risk, (2) addressing monitoring requirements across the organization, (3) identifying the minimum monitoring frequency for implemented security controls across the organization, (4) defining the ongoing control assessment approach, (5) describing how ongoing assessments are to be conducted, (6) defining security reporting requirements and recipients of the reports, and (7) authorizing the strategy for approval by the senior accountable official for risk management or the risk executive (function).

- addressing monitoring requirements across the organization,
- defining the ongoing control assessment approach, and
- defining security reporting requirements.

NNSA did not include these elements for organization-wide cybersecurity risk management in its continuous monitoring strategy because it was not using the latest guidance from NIST.⁴⁴ In May 2022, NNSA officials acknowledged that gaps exist in fully implementing this practice and attributed these gaps to competing priorities and resource constraints, such as allocating personnel resources to address existing cybersecurity matters and responding to ongoing audits and other mission obligations. Without developing a comprehensive continuous monitoring strategy that includes all elements from NIST guidance, NNSA is likely to lack a clear understanding of the organization's cybersecurity posture and limit its ability to respond to emerging cyber threats in an effective manner.

Until NNSA fully implements foundational cybersecurity risk management practices in its traditional IT environment, it will be limited in its ability to establish clear and up-to-date cybersecurity expectations, understand its organization-wide cybersecurity posture, and respond to emerging cyber threats across the organization. More details on NNSA's implementation of the six foundational risk management practices in the traditional IT environment are provided in appendix II.

M&O Contractors' Implementation of Foundational Practices for Traditional IT

Each of the seven M&O contractors fully implemented three of the six foundational risk management practices in the traditional IT environment:

- Practice 3: Document and maintain cybersecurity program policies and plans.
- Practice 4: Assess and update organization-wide cybersecurity risks.
- Practice 5: Designate controls that are available for information systems or programs to inherit.⁴⁵

⁴⁴In December 2018, NIST revised its risk management framework to include additional steps for organizations in preparing for risk management.

⁴⁵Apps. V through VII provide further details on our analyses.

For example, we found that all of the M&O contractors had maintained organization-wide cybersecurity program plans. All of the contractors also assessed and updated organization-wide cybersecurity risks by documenting assessment results in various sources, such as site-wide risk assessment reports and individual improvement plans. In addition, M&O contractors designated controls that are available for information systems or programs to inherit in various sources, such as site-wide cybersecurity program plans and policies, common control catalogs, and individual system security plans. However, M&O contractors varied in their implementation of the other three practices:

- **Identify and assign cybersecurity risk management roles and responsibilities (practice 1).** Of the seven M&O contractors, two—Pantex/Y-12 and Savannah River—fully implemented this foundational practice; four—Lawrence Livermore, Los Alamos, Nevada Site, and Sandia—substantially implemented it; and one—Kansas City—partially implemented the practice.

For example, we found that the Kansas City contractor only partially implemented this practice because its risk-based documents (e.g., site *Cyber Security Program Plan* and *Site Specific Risk Management Plan*) did not identify and assign certain key cybersecurity risk management roles and responsibilities recommended by NIST. The four key roles that were not identified were (1) the site's authorizing official designated representative, (2) the risk executive, (3) the chief information officer, and (4) the senior accountable official for risk management. Furthermore, the contractor did not assign a key role—a senior accountable official for risk management—to a specific individual or group to guide and oversee its risk management program. In May 2022, contractor representatives acknowledged gaps in this practice and attributed the deficiencies to budget and personnel resource constraints. Representatives said they expect to address these deficiencies by the end of calendar year 2022. By not identifying and assigning cybersecurity risk management roles and responsibilities, as described by NIST, the contractor at Kansas City has limited its effectiveness in managing site-wide risk.

Furthermore, the contractors managing Lawrence Livermore, Los Alamos, the Nevada Site, and Sandia had not identified the roles and responsibilities of the authorizing official designated representative in their respective site's cybersecurity program plans. It is important to designate the role of the authorizing official's designated representative because they are empowered to act on behalf of the

authorizing official to coordinate and conduct the day-to-day activities associated with managing risk. Appendix III provides further details on our analysis of contractors' implementation of this practice.

- **Establish and maintain a cybersecurity risk management strategy for the site (practice 2).** Four of the seven M&O contractors—Kansas City, Lawrence Livermore, the Nevada Site, and Pantex/Y-12—fully implemented this foundational practice; two—Los Alamos, Sandia—substantially implemented it; and one—Savannah River—partially implemented it.

For instance, the contractor managing NNSA operations at Savannah River had not maintained its strategy to account for organizational changes, as required. Specifically, in May 2022, the contractor provided a March 2022 Operational Risk and Opportunity Report as evidence of a NNSA-focused risk management strategy. However, this report focused on an assessment of cybersecurity risk and did not reflect the contractor's review of its risk management strategy.

The Savannah River contractor documented a cybersecurity risk management strategy through its October 2016 *Savannah River Risk and Opportunity Management Plan*. Contractor representatives told us this strategy document is managed by DOE's Office of Environmental Management. However, this strategy was not incorporated into NNSA's March 2022 Operational Risk and Opportunity Report. Moreover, inconsistent with NIST and CNSS guidance, this contractor had not performed an annual review of its strategy or updated it for over 5 years. Savannah River contractor representatives told us that DOE's Office of Environmental Management does not require its M&O contractors to perform such reviews. The representatives stated, however, that the contractor planned to review and update the Savannah River Risk and Opportunity Management Plan later in calendar year 2022.

By not maintaining a risk management strategy that accounts for organizational changes, as called for by NIST and CNSS, the Savannah River contractor has less assurance that they will have a site-wide understanding of risks and appropriate risk response strategies to protect its systems and data.

In addition, the contractors operating Los Alamos and Sandia each established a site-wide risk management strategy, but their strategies did not address all of the elements from NIST guidance. According to

NIST guidance, it is important that a risk management strategy address all elements to inform how cybersecurity risk is framed, assessed, responded to, and monitored. Appendix IV provides further details on our analysis of contractors' implementation of this practice.

- **Develop and maintain an organization-wide continuous monitoring strategy (practice 6).** Four of the seven M&O contractors—Lawrence Livermore, Los Alamos, Pantex/Y-12, and Sandia—substantially implemented this foundational practice; one—Savannah River—partially implemented it; and two—Kansas City and the Nevada Site—minimally implemented this practice.

NNSA officials attributed shortfalls in its M&O contractors' ability to develop and maintain site-wide continuous monitoring strategies to the same impediments as discussed above. By not developing and maintaining a comprehensive continuous monitoring strategy that includes all elements from NIST guidance, the contractors at the Savannah River, Kansas City, and Nevada sites lack a clear understanding of their site-wide cybersecurity postures and are limited in their ability to respond to emerging cyber threats in a timely manner. Specifically, at these three sites we found the following:

- The M&O contractor at Savannah River developed a site-wide continuous monitoring strategy in its March 2020 *Continuous Monitoring Plan for the NNSA Savannah River Field Office Authorization Boundaries* that addressed most of the elements from the NIST guidance, such as defining security reporting requirements and minimum monitoring frequencies. However, the contractor had not maintained the strategy to address cybersecurity risks and requirements across the organization. Specifically, the contractor had not defined any update frequency and had not updated its strategy in over 2 years. In March 2022, contractor representatives attributed the gaps in maintaining its continuous monitoring strategy to competing priorities, such as the implementation of business projects that exhausted personnel resources. They also stated that the strategy is undergoing a review and an update, with a planned completion date by September 2022.

In addition, we found that the contractor's strategy did not address two elements—describing considerations for supply chain risk and how ongoing risk assessments are to be conducted—from NIST guidance in its strategy. Regarding the first element, we found that the contractor's requisition security review process described

considerations for supply chain risk.⁴⁶ However, the contractor did not address this element in its continuous monitoring strategy, as recommended by NIST. Moreover, the contractor did not provide evidence that addressed the second missing element—describing how ongoing risk assessments are to be conducted. Addressing these elements in an organization’s continuous monitoring strategy make it more robust and comprehensive. In May 2022, Savannah River contractor representatives stated that the contractor expects to update the strategy to include the missing elements from NIST guidance once modifications to its contract are completed.

- M&O contractors at the Kansas City and the Nevada sites minimally developed and maintained site-wide continuous monitoring strategies. Kansas City’s contractor provided a September 2019 Site Specific Risk Management Plan, and Nevada’s contractor provided its August 2019 Continuous Monitoring Policy. Each site also provided documentation related to the execution of continuous monitoring activities, such as continuous monitoring status reports and metrics. Contractor representatives at each site told us that they believed that, taken together, this documentation constituted a continuous monitoring strategy.

However, this documentation was not consistent with the continuous monitoring practice in a number of ways. The documentation provided by both sites addressed one element of a comprehensive, site-wide continuous monitoring strategy from NIST guidance—defining monitoring requirements across the organization. At the same time, the contractor documentation did not address other elements, such as defining security reporting requirements and identifying the minimum monitoring frequencies for implemented security controls across the organization. In addition, the execution of continuous monitoring activities does not replace the need for a strategy that defines the activities that should occur, ongoing assessment approaches, and the frequency of monitoring.

Contractor representatives at Kansas City stated that the contractor expects to complete development of a strategy by

⁴⁶The requisition security review process includes activities that involve stakeholder coordination aimed at developing and integrating supply chain risk management tools into the site’s procurement process.

September 2022. Contractor representatives at the Nevada Site first stated that they had no plans to develop a strategy and would continue to rely on existing documentation. However, after reviewing a draft of our report, contractor representatives stated that they had decided to change their approach and that they would develop a documented continuous monitoring plan to address all elements of the NIST guidance.

In addition, the contractors managing Lawrence Livermore, Los Alamos, Pantex/Y-12, and Sandia established continuous monitoring strategies, but these strategies did not fully address all of the elements from NIST guidance. To better prepare an organization to respond to emerging cyber threats in an efficient and cost-effective manner, a continuous monitoring strategy should be comprehensive and address all elements to better prepare an organization for responding to risk, in accordance with NIST guidance. Appendix VIII provides further details on our analysis of contractors' implementation of this practice.

Until NNSA's M&O contractors fully implement foundational cybersecurity risk management practices in the traditional IT environment, they will have less assurance that their understanding and response to cybersecurity risks is effective. Because the M&O contractors execute many aspects of NNSA's missions, their incomplete implementation of foundational risk management practices will limit NNSA's ability to assert that comprehensive cyber risk management framework exists for its nuclear security enterprise.

NNSA Has Not Implemented Any of the Foundational Risk Management Practices for OT

NNSA has made limited progress—after several years of effort—to implement foundational risk management practices that address OT cybersecurity at the organizational level in part because NNSA has not identified the resources necessary to achieve full implementation. As a

result, NNSA has not yet fully implemented any of the foundational risk management practices in the OT environment.⁴⁷

NNSA is currently managing OT cybersecurity under the risk management program and policies that the agency developed for traditional IT, a practice that is at odds with NIST guidance and DOE requirements. NIST guidance recommends and DOE Order 205.1C requires NNSA to implement foundational risk management practices that are specifically tailored to address OT cybersecurity as part of a comprehensive cybersecurity risk management program.⁴⁸

According to NIST, OT systems often require different approaches when selecting and managing risk. For example, according to NIST guidance, OT systems are often managed by control engineers rather than IT personnel, and they may lack features that traditional IT systems have such as encryption, error logging, and password protection. Consequently, OT systems may require different approaches when selecting and implementing cybersecurity safeguards or compensating controls for their unique circumstances, such as network segmentation. NNSA officials acknowledged that there are weaknesses in managing OT under a cybersecurity program developed to address traditional IT risks.

NNSA officials told us that they began an initiative in the fall of 2018—now titled Operational Technology Assurance (OTA)—to implement the foundational risk management practices to address risks in the OT environment at NNSA and its sites. Since 2018, NNSA and its M&O contractors have taken some actions as a precursor to or as part of the OTA initiative. For example, NNSA officials told us that they had surveyed senior management within NNSA and at each of NNSA's sites to identify the highest priority mission-impact OT functions at each site and to implement measures to address them. In addition, NNSA officials told us that they had undertaken efforts to capture OT best practices within and outside NNSA's nuclear security enterprise, established partnerships with

⁴⁷During our review, NNSA was developing but did not have OT guidance for contractors to implement a cybersecurity risk management framework. Therefore, our review focused on NNSA's organization-level efforts.

⁴⁸National Institute of Standards and Technology, *Guide to Industrial Control Systems Security*, NIST SP 800-82, Revision 2 (Gaithersburg, Md.: May 2015).

the broader OT community, and developed and held two courses to train site staff on OT considerations and potential risks.⁴⁹

We also found that NNSA has taken actions that align with and could be consistent with two foundational risk management practices, when fully implemented:

- **Document and maintain cybersecurity program policies and plans (practice 3).** NNSA has undertaken actions to revise policies and plans that could be consistent with this practice when they are issued. First, NNSA officials told us that they are taking action to identify all the orders, supplemental directives, and policy documents that may need to be revised to incorporate tailored requirements specific to the OT cybersecurity environment. NNSA officials told us that they are primarily focusing on revising NNSA's *Cybersecurity Program Plan* and SD 205.1 *Baseline Cybersecurity Program* to address the OT cybersecurity environment. In October 2021, NNSA issued its revised *Cybersecurity Program Plan* to define OT and place OT systems within the scope of the enterprise's cyber-based security environment. In addition, the draft version of SD 205.1 we reviewed, dated April 2022, includes a requirement for NNSA to improve and maintain a cybersecurity program that covers the implementation and maintenance of information security configuration and vulnerability management security controls for OT systems. However, as previously discussed, NNSA officials did not have an estimated completion date for this directive. NNSA officials said that other documents would likely need to be revised and that they were still attempting to identify the remaining scope of documents for revision.

Second, NNSA developed an *OTA Guidebook for NNSA* and the sites to determine gaps in the current OT systems and risk approaches. The March 2022 version of the guidebook, which we reviewed, presents a systematic process for identifying, assessing, and managing OT digital risk. The guidebook states that it is a tool for aligning policy, business, and technological approaches to OT cybersecurity. NNSA officials told us that the guidebook was being used by all NNSA sites to secure the highest-priority mission impact OT risks at each site. In June 2022, NNSA officials stated that the guidebook was updated nearly monthly to incorporate lessons learned. When used to address all OT risks at all sites, this guidebook

⁴⁹In addition, within Defense Programs, NNSA established the Nuclear Weapon Digital Assurance activity to, among other things, address the risks of digital subversion to nuclear weapon manufacturing and testing capabilities.

could be another action consistent with the practice of documenting and maintaining cybersecurity risk-based plans and policies.

- **Assess and update organization-wide cybersecurity risks (practice 4).** NNSA has undertaken two studies that have broadly assessed organization-wide OT cybersecurity risks. First, NNSA commissioned a study by the JASON—an independent scientific advisory group—to identify vulnerabilities in the OT environment and develop recommendations to minimize and mitigate these vulnerabilities.⁵⁰ The report, dated January 2020, included 13 recommendations to improve NNSA’s OT cybersecurity posture—six near-term and seven longer-term recommendations. In December 2021, NNSA officials told us that the agency OTA Guidebook addressed these recommendations. NNSA also commissioned a private, nonprofit corporation, the Institute for Defense Analyses, to further examine IT and OT challenges at five NNSA sites.⁵¹ In March 2022, the institute issued its study to NNSA, which included a number of recommendations for NNSA to improve IT and OT cybersecurity risk management. As of May 2022, NNSA officials stated that they are in the process of reviewing these recommendations.

Notwithstanding these efforts, NNSA officials told us that they did not have an overall plan or roadmap to guide its future actions on OT cybersecurity—including efforts to provide guidance and expectations to M&O contractors operating the sites—and to ensure that those actions will be consistent with the foundational risk management practices. In written answers provided in September 2021, NNSA officials told us that the OTA initiative is still considered to be in its “inception” phase after 3 years and said that resources have not been sufficient to support a robust OT cybersecurity risk management program. The March 2022 Institute for Defense Analyses study concluded that NNSA does not appear to have a nuclear security enterprise-wide approach to securing OT and emphasized that NNSA needs OT policies and standards. This study also cited evidence that NNSA’s Office of Information Management may be

⁵⁰The JASON’s mission is to contribute to national security and public benefit by working on problems of importance to the U. S. government. The group is organized and supported by the MITRE Corporation—a not-for-profit research and development organization.

⁵¹Institute for Defense Analyses, *Independent Cybersecurity Assessment of the National Nuclear Security Administration (NNSA) Information and Operational Technology (IT & OT) Systems and Programs*, IDA Paper P-33028 (Alexandria, Va.: March 2022). The five sites were Sandia, Los Alamos, Kansas City, Savannah River, and Lawrence Livermore.

severely understaffed in general—a situation that could contribute to a shortage of resources to direct to the OTA initiative.

NNSA officials said that they had not produced documentation—such as a business case—typically used to justify the allocation of resources for a new initiative. NNSA officials told us that they had used the JASON report and the site mission impact prioritization to inform an initial resource request to support the OTA initiative. NNSA officials also stated that they hoped that our report would provide support for additional resources.

In February 2022, NNSA officials noted that requested funding for OT cybersecurity in fiscal year 2023 is divided between budget justifications for its Office of Information Management and Office of Defense Programs but could not state how much of the requested funding from each would go to OTA.⁵² In May 2022, NNSA officials said that for a number of needs that they had identified for inclusion in the fiscal year 2023 budget request—only some—for personnel training, procurement of technical tools, and one additional staff person—were ultimately included. These officials stated that they had developed a funding target for fiscal year 2024 as part of the programming phase of NNSA’s fiscal year 2024 budget development process, but they were unable to specify the target or provide supporting documentation for the target because of the ongoing budget development process.

If the OTA initiative is funded in fiscal year 2024, NNSA officials told us that they plan to conduct an inventory and categorization of OT systems across the sites, procure additional tools and storage capacity, and hire two additional staff.⁵³ However, NNSA officials said that the office now expected a reduction in funding in fiscal year 2024 and that they were not sure how many of these items they would be able to complete.

A May 2021 executive order states that the federal government must bring to bear the full scope of its authorities and resources to protect and secure its OT systems.⁵⁴ Further, NIST guidance and NNSA policy

⁵²In written answers provided in February 2022, NNSA officials indicated that Defense Programs would use some funding to assist with OT activities.

⁵³NNSA officials estimated that there are over 200,000 unique pieces of OT equipment across the nuclear security enterprise and that one site—Kansas City—has approximately 46,000 pieces of OT equipment.

⁵⁴Executive Order 14028.

provide direction to agency activities that require additional funding.⁵⁵ Specifically, NIST guidance for the cybersecurity of industrial controls systems (which is a subset of OT systems) recommends the development of a business case to provide an understanding of the high-level process to implement, operate, and maintain a risk management program; costs and resources required; benefits of such a program; and cost of not implementing such a program.⁵⁶ Such a business case could be used to identify future OTA resource needs and potential funding levels for consideration in NNSA's annual planning, programming, budgeting, and evaluation process, which is the framework that NNSA uses to prioritize and fund program activities to meet agency goals.

Delineating clear funding for OT cybersecurity could elevate the priority for this environment above the current hybrid funding arrangement where it may compete with other programmatic resource needs. In addition, providing a clear stream of funding would serve to distinguish OT cybersecurity as a discrete programmatic activity and demonstrate NNSA's commitment to securing OT.

NNSA Is Making Progress toward Implementing Most Foundational Cybersecurity Risk Management Practices for NW-IT

NNSA has implemented one foundational cybersecurity risk management practice to address NW-IT cybersecurity and is making progress toward implementing most additional practices.⁵⁷ Recognizing that greater effort was needed to bring NW-IT cybersecurity into line with foundational risk management practices, NNSA began an initiative—called Nuclear Weapon Digital Assurance (NWDA)—in 2019 to implement a risk

⁵⁵National Nuclear Security Administration, *Planning, Programming, Budgeting, and Evaluation (PPBE) Process*, Policy 103.1B (Washington, D.C.: May 21, 2021).

⁵⁶NIST SP 800-82.

⁵⁷During our review, NNSA was developing, but did not have, tailored NW-IT guidance for contractors to implement a cybersecurity risk management framework. Therefore, our review focused on NNSA's organization-level efforts.

management framework for the NW-IT environment consistent with NIST guidance.⁵⁸

Prior to this initiative, NNSA had managed cybersecurity risks to NW-IT since 2015 through its Nuclear Enterprise Assurance process, which provided a general framework for managing risks to weapons but did not specifically address NW-IT cybersecurity. NNSA officials overseeing the NWDA initiative told us that they were initially able to carve out funding from existing Defense Programs' resources and obtain staff from one of NNSA's sites to assist with implementation of the initiative. This funding and staff provided the NWDA initiative with the initial resources to develop a July 2020 roadmap and begin implementing NIST's initial risk management practices.

In October 2021, NNSA established the Nuclear Enterprise Assurance (NEA) Division as a new sub-office within Defense Programs to manage the NWDA initiative. In January 2022, NNSA also issued SD 452.4-1, *Nuclear Enterprise Assurance*, which established requirements to ensure consistent and coordinated NNSA and contractor application of NEA principles to nuclear weapons programs and nuclear-weapons enabling capabilities, among other things.⁵⁹ In NNSA's fiscal year 2023 budget request to Congress, NNSA requested funding of \$48.9 million for the new NEA subprogram, stating that it would be used to prevent, detect, and mitigate subversion risks to the nuclear weapons stockpile and associated design, production, and testing capabilities. If funded, the NEA Division would use this funding line to implement planned NW-IT activities and nuclear weapon-related OT activities, NNSA officials told us.

⁵⁸Efforts associated with NWDA began in early 2019, but the official start of NWDA activities was delayed until Information Management delegated authority for NW-IT to the Office of Defense Programs in October 2019. The NWDA initiative also addressed implementing a risk management framework in the OT environment.

⁵⁹National Nuclear Security Administration, *Nuclear Enterprise Assurance*, SD 452.4-1 (Washington, D.C.: Jan. 27, 2022). According to this directive, NEA is NNSA's program to prevent, detect, and mitigate potential consequences of subversion, including unauthorized acts that may lead to denial of authorized use or degradation of weapon reliability or performance. NEA is intended to reduce the risk of subversion by advanced persistent threats and other adversaries that possess the expertise and resources that enable them to create and exploit subversion opportunities. NEA includes the systematic identification, assessment, and mitigation of subversion risks, based on analysis of vulnerabilities and adversarial threats, to provide assurance that nuclear weapons, nuclear weapons-related capabilities, and related crosscutting functions and programs are not subverted or compromised.

NNSA officials stated that NNSA intends to fully implement activities in the NW-IT environment that will be consistent with foundational cybersecurity risk management practices. However, this process has been delayed. According to NNSA documentation, NNSA originally planned to complete implementation of the NIST risk management framework in the NW-IT environment by March 2022; however, in May 2022, NNSA officials stated that they were revising their implementation roadmap and that activities would likely extend into calendar year 2024. NNSA officials attributed the delays in NW-IT implementation to ongoing hiring challenges but stated that they had hired one new staff in October 2021 and planned to hire two new staff members in June 2022 and October 2022.

As of March 2022, NNSA had fully implemented one practice in the NW-IT environment consistent with foundational risk management practices. Specifically, NNSA had identified and assigned cybersecurity risk management roles and responsibilities (practice 1) for this environment.⁶⁰ NNSA officials told us that activities consistent with implementation of four of the remaining five foundational risk management practices were underway but not complete:

- **Document and maintain cybersecurity program policies and plans (practice 3).** Consistent with the intent of this practice, NNSA officials have issued one revised policy document and are revising a second to address NW-IT. Specifically, in January 2022, NNSA issued its revised NEA directive in SD 452.4-1, which contains specific language acknowledging the threats posed by cybersecurity and supply chain vulnerabilities and requires the development and application of a risk management methodology to counter such threats. The methodology is to include assessing cyber threats, identifying potential security controls and measures to counter such threats, and integrating with NNSA's existing risk management processes to help inform risk-based decisions. In addition, we reviewed NNSA's April 2022 draft version of SD 205.1 and found that it addresses NW-IT risk management—in contrast to the current version, which does not address NW-IT.

However, as previously discussed, in May 2022, NNSA officials stated that they did not have an estimated completion date for SD 205.1. According to an internal NNSA memorandum, the new NEA division

⁶⁰Specifically in the NW-IT environment, NNSA had assigned leadership within Defense Programs to cybersecurity risk management roles, such as the authorizing officials, risk executive function, and senior information security officer.

will continue the existing work to integrate the risk management framework into NNSA's nuclear weapon acquisition life cycle system engineering processes, requirements, and policies, and NNSA has identified a list of additional policies to update. However, the documentation does not specify a target time frame for integrating the NIST risk management framework into these NNSA processes.

- **Assess and update organization-wide cybersecurity risks (practice 4).** NNSA has not conducted an organization-wide cybersecurity risk assessment that addresses the NW-IT environment's risks. However, consistent with the initial steps of this practice, NNSA officials stated that they had identified and validated a set of NW-IT baseline controls for stockpile modernization systems in October 2021. In May 2022, NNSA officials told us that they initially planned to conduct a second gap analysis of NW-IT controls for stockpile sustainment systems from January 2022 through June 2022 but had encountered delays. They now expect to complete this analysis by the middle of calendar year 2023. According to NNSA's NW-IT controls baseline document, identification of such controls is the first step in preparation to conduct an organization-wide cybersecurity risk assessment for NW-IT. After completion of this step, NNSA will likely be better prepared to identify cyber risks in the NW-IT environment.
- **Designate controls that are available for information systems or programs to inherit (practice 5).** NNSA officials told us that they had identified a set of baseline controls for the NW-IT environment, which contain security controls that are available for inheritance consistent with this practice, but the designation of these controls was not comprehensive. NNSA identified and documented 23 program management-related security controls that are available for inheritance, such as system inventory, insider threat program, and risk management strategy. However, this document does not designate controls that are available for information systems or programs to inherit, as recommended by NIST, such as security assessment, continuous monitoring, and baseline configuration (i.e., a documented set of specifications for an information system).
- **Develop and maintain an organization-wide continuous monitoring strategy (practice 6).** NNSA had not yet developed a NW-IT continuous monitoring strategy and, according to NNSA's baseline control documentation, had not defined organizational requirements for continuous monitoring in the NW-IT environment. NNSA officials told us that efforts to develop a weapons continuous monitoring strategy and some guidance were in draft but did not

provide this documentation to us. NNSA officials said that before developing a strategy, they would first conduct a gap assessment of each of the selected controls and existing surveillance engineering practices on a system-by-system basis. However, NNSA's focus on system-level risk management does not address the need for an organization-wide strategy for continuous monitoring. Organization-wide strategies for continuous monitoring are important because they establish methods for examining an organization's risk posture and the collective effectiveness of controls across its various systems and business processes on an ongoing basis.

NNSA has not taken action consistent with the establishment and maintenance of a cybersecurity risk management strategy for the organization (i.e., practice 2) in the NW-IT environment. In February 2022, NNSA officials stated that the agency's NW-IT organization-wide risk management strategy was addressed by DOE orders and NNSA supplemental directives, such as the revised NEA directive SD 452.4-1 and the draft version of SD 205.1. NNSA officials further stated that requirements for nuclear weapons risk management are maintained in the Defense Programs' Business Processes System—which contains additional business requirements, processes, and tools for managing nuclear stockpile work.

However, according to NIST guidance, an agency's policies—such as NNSA's supplemental directives—and processes—such as those maintained in the Business Processes System—may provide input into the establishment of a risk management strategy but should not constitute it. We found that both SD 452.4-1 and the April 2022 draft version of SD 205.1 did not address all elements from NIST guidance, such as describing considerations for supply chain risk, determining the methodology for conducting a risk assessment, and having a strategy for responding to cybersecurity risks. In addition, the business requirements, processes, and tools we reviewed did not address risk management strategy elements from NIST guidance. Without establishing and maintaining a risk management strategy, as called for in CNSS guidance, NNSA is likely to lack an organization-wide understanding of acceptable risk levels and appropriate risk response strategies to assess and plan for cyber threats to its NW-IT systems and data.

Contractor-Required Monitoring of Subcontractor Cybersecurity Is Inconsistent

M&O contractors are required—under provisions of their contracts that incorporate DOE and NNSA cybersecurity requirements—to monitor subcontractor cybersecurity measures. However, we found that M&O contractors do not consistently monitor subcontractor cybersecurity measures because some do not believe they are required to do so. In addition, NNSA does not emphasize the importance of M&O oversight of subcontractors' cybersecurity through its annual contractor performance assessment process. NNSA officials have plans that could enhance contractor and subcontractor cybersecurity requirements by implementing a standardized cybersecurity framework for unclassified systems, but implementation of this framework is likely to be significantly delayed.

M&O Contractors Are Not Consistently Monitoring Subcontractor Cybersecurity Measures

NNSA's SD 205.1, Baseline Cybersecurity Program—incorporated into each M&O contractor's contract with NNSA—contains a contractor requirements document that specifically requires M&O contractors to ensure that subcontractors comply with NNSA cybersecurity requirements. Thus, NNSA does not directly oversee how subcontractors implement cybersecurity measures because general subcontractor oversight is the responsibility of the M&O contractors. Representatives from each of the M&O contractors told us that they complied with the requirement by including cybersecurity provisions in their subcontracts.⁶¹

However, through interviews and written responses from representatives of each of the seven M&O contractors, we found that once a subcontract was awarded, M&O contractors' monitoring of such measures was inconsistent among the sites. Specifically, representatives of two M&O contractors—those operating the Sandia and Y-12/Pantex sites told us that they conduct frequent subcontractor monitoring or are implementing a process to do so. Contractor representatives for Lawrence Livermore said that they conduct such monitoring annually, or on another defined

⁶¹In August 2021, NNSA identified 12 different subcontractors that provided IT-related goods and services in fiscal year 2020. However, this list only reflected the subcontractors for a single M&O contractor operating the Pantex and Y-12 sites.

interval for some services, and intended to implement further oversight processes.

However, M&O contractor representatives at Kansas City, Los Alamos, and the Nevada Site told us that they are not contractually obligated to monitor how subcontractors implement cybersecurity measures. Specifically, contractor representatives from Kansas City told us that they had no contractual requirement to conduct oversight of a subcontractor's cybersecurity practices. They further stated that their budget is tightly controlled by NNSA and that risk-based decisions—made by or involving the senior NNSA information system official on site—have to be made to stay within that budget and that the focus is on protecting NNSA systems rather than subcontractor systems.

Los Alamos representatives stated that they requested security plans from subcontractors and conducted follow-up interviews to review security measures. They further stated that they do not have the resources to check the risk management posture of all vendors, but they try to prioritize subcontracts that include access to classified networks or sensitive information.

Contractor representatives from the Nevada Site told us that the site does not need to conduct active oversight of subcontractors because it requires subcontractors to use Nevada Site systems to conduct work that includes sensitive federal information. The Nevada Site's *Cyber Security Program Plan*, which NNSA requires for all sites, does not include any reference to subcontractors' use of Nevada Site systems to conduct work with sensitive federal information, or discussion of this practice as a risk mitigation measure. Contractor representatives stated that this oversight approach was addressed in other site documentation. However, we could not corroborate NNSA's acceptance of its oversight approach because no documents were provided to us to support the contractor's position.

Because M&O contractors are not consistently performing required monitoring subcontractor cybersecurity measures, NNSA has little assurance that contractors are complying with their contractual requirement to ensure subcontractor compliance with NNSA cybersecurity requirements. As a result, information and systems provided or maintained by subcontractors may not be effectively protected against cybersecurity risks. DOE's Office of Acquisition Management often issues a "policy flash" to transmit information and items of interest to DOE and NNSA and could be a potential avenue for DOE and NNSA to clarify and reinforce M&O contractor responsibilities.

Reinforcement of the M&O contractors' contractual requirement to oversee subcontractor cybersecurity by NNSA, such as through a policy flash or other method, could result in more consistent oversight and more effective protection.

NNSA Does Not Assess Contractor Oversight of Subcontractor Cybersecurity Measures through Its Performance Evaluation Process

In March 2019, we reported that most—21 out of 24—of DOE and NNSA annual performance assessment plans that we reviewed did not contain any explicit performance criteria to assess contractor oversight and management of subcontractors.⁶² At that time, DOE officials said that the contractor is responsible for completing the scope of work in the contract, regardless of whether it was performed by the contractor or a subcontractor. We recommended that DOE include such explicit performance criteria because it would provide DOE with more reasonable assurance that the agency is emphasizing the importance of subcontract management and provide contractors with an additional incentive to properly manage their subcontractors. DOE partially concurred with this recommendation but, as of April 2022, held that sufficient guidance existed for contracting officers to make informed decisions on whether to include contractor management of subcontractors as part of the annual assessment process.

With regard to specific contractor oversight of subcontractor cybersecurity measures, in March 2021, officials from NNSA's Office of Acquisition and Project Management affirmed that NNSA did not assess contractors on such oversight. However, a senior official stated in a later meeting that NNSA would begin to do so immediately.

As of January 2022, NNSA officials within the Office of Acquisition and Project Management could not answer whether they had done so and did not produce documentation that such a criterion had been added to the annual performance evaluation process. These officials stated that current performance criteria—under which M&O contractors are generally evaluated on the extent to which they deliver efficient, effective and responsive IT systems and cybersecurity—were sufficient.

⁶²[GAO-19-107](#).

As previously discussed, there are gaps in M&O contractors' implementation of required monitoring of subcontractor cybersecurity measures. NNSA could emphasize the importance of subcontractor cybersecurity measures, and the importance of M&O contractors monitoring such measures, by including specific performance criteria in the annual M&O contractor performance evaluation process. By doing so, NNSA would have greater assurance that information to which the contractor and subcontractor have access or custody is being protected by contractors and subcontractors, as required.

NNSA Has Plans That Could Enhance Subcontractor Cybersecurity Requirements, but Implementation Could Be Significantly Delayed

The contractor requirements document attached to the April 2022 draft version of SD 205.1, *Baseline Cybersecurity Program*, contains two proposed requirements for NNSA contractors and subcontractors to implement essentially the same standardized cybersecurity framework. The first would require contractors and subcontractors to implement NIST SP 800-171 and have that implementation certified by a third party no more than 18 months after the contractor requirements document is incorporated into the M&O contract. Under the second requirement, NNSA would require contractors and subcontractors to have their implementation of CMMC level 2—the advanced level—verified by a third party no more than 24 months after the contractor requirements document is incorporated into the M&O contract.⁶³ As previously discussed, CMMC largely adopts the requirements of NIST SP 800-171 and, thus, these proposed requirements overlap.

According to DOD, regular cybersecurity assessments of contractors are intended to provide increased assurance that sensitive information is adequately protected. NNSA's proposed adoption of NIST SP 800-171 and CMMC, and third-party verification of such measures, could address some inconsistencies among the M&O contractors in their required oversight of subcontractors that handle unclassified information. However, in May 2022, NNSA officials told us that they did not have an estimated completion date for SD 205.1—a directive that has not been updated in 5 years. As previously discussed, SD 251.1B, *Directives*

⁶³This requirement is contingent on DOD having implemented CMMC.

Management, requires the organization to review directives such as SD 205.1 every 3 years.

It is also unclear when DOD will fully implement CMMC. DOD began implementation of CMMC in November 2020 under a 5-year pilot phase and planned to pilot the CMMC requirement on up to 15 acquisitions in fiscal year 2021. We recently reported that DOD had not included the requirement in any acquisitions that year in part because of delays in certifying third-party assessors.⁶⁴ Furthermore, in November 2021, DOD announced that it was heavily revising the CMMC framework and had suspended the pilot to implement the revised framework. Given these delays, it is unclear how the M&O contractors and their subcontractors will be able to implement CMMC before DOD has progressed further in its pilot, including the certification of sufficient third-party assessors.

As discussed above, over the course of our review, NNSA delayed the SD 205.1 completion date several times, and NNSA officials did not have an estimated completion date as of May 2022. In light of the increasing threat to systems with federal information, NNSA needs to have greater assurance that contractors and subcontractors are implementing a standardized cybersecurity framework. Including a requirement for third-party validation of cybersecurity measures in SD 205.1 would provide NNSA additional assurance that contractors and subcontractors are addressing the agency's expectations for cybersecurity.

Conclusions

NNSA and its M&O contractors have made strides in implementing most of the foundational cybersecurity risk management practices in NNSA's traditional IT environment. However, the agency's implementation is not complete or consistent in many foundational risk management practices. Until NNSA fully implements foundational cybersecurity risk management practices in its traditional IT environment, management and M&O contractors have a limited ability to establish clear and up-to-date cybersecurity expectations and respond to emerging cyber threats across the organization.

The OT environment is vast and highly complex, encompassing hundreds of thousands of systems potentially at risk. However, NNSA's OTA

⁶⁴[GAO-22-104679](#).

initiative is still in its inception phase after 3 years and is proceeding at a pace out of sync with the potential scope and severity of the cybersecurity risk present in this environment. By creating a business case for the OTA activity that it can feed into NNSA's existing budgeting process, NNSA will be better positioned to marshal the attention and resources necessary to develop an OT cybersecurity risk management framework that aligns with foundational risk management practices—a vital activity of national security interest.

NNSA also faces a complex task in implementing the foundational risk management practices in the NW-IT environment. While NNSA has undertaken some activities to implement foundational cybersecurity practices, the current policies fall short of a comprehensive risk management strategy for the NW-IT environment. Without such a strategy, NNSA may lack an organization-wide understanding of acceptable risk levels and appropriate risk response strategies to assess and plan for cyber threats to its NW-IT systems and data.

NNSA has an urgent need to swiftly ensure M&O contractor oversight of subcontractor cybersecurity. However, NNSA has yet to clarify to contractors that they are required to monitor subcontractor cybersecurity measures, include an evaluation of that oversight in its annual contractor performance assessment process, or implement third-party validation of subcontractor cybersecurity measures. By doing so, NNSA could close gaps in M&O contractor monitoring of subcontractors and in NNSA's limited information about such oversight. Furthermore, NNSA would have greater assurance that information handled by contractors and subcontractors is consistently and effectively protected.

Recommendations

We are making the following nine recommendations:

The NNSA Administrator should promptly finalize its planned revision of Supplemental Directive 205.1, Baseline Cybersecurity Program, to include the most relevant federal cybersecurity requirements and review the directive at least every 3 years. (Recommendation 1)

The NNSA Administrator should direct NNSA's Office of Information Management, and the site contractors that have not done so, to develop and maintain cybersecurity continuous monitoring strategies that address all elements from NIST guidance. (Recommendation 2)

The NNSA Administrator should direct NNSA's Office of Information Management, and the site contractors that have not done so, to identify and assign all risk management roles and responsibilities called for in NIST guidance. (Recommendation 3)

The NNSA Administrator should direct that the site contractors that have not done so maintain a site-wide cybersecurity risk management strategy that addresses all elements from NIST guidance and perform periodic reviews at least annually. (Recommendation 4)

The NNSA Administrator should direct the Office of Information Management to identify the needed resources to implement foundational practices for the OT environment, such as by developing an OT activity business case for consideration in NNSA's planning, programming, budgeting, and evaluation process. (Recommendation 5)

The Director of NNSA's Office of Defense Programs should establish a cybersecurity risk management strategy for nuclear weapons information technology that includes all elements from NIST guidance. (Recommendation 6)

The Director of NNSA's Office of Acquisition and Project Management should clarify and reinforce to the M&O contractors, such as by a policy flash or other communication, that they are required to monitor subcontractor's cybersecurity measures. (Recommendation 7)

The Director of NNSA's Office of Acquisition and Project Management should include performance criteria evaluating contractor oversight of subcontractor cybersecurity measures in the annual M&O contractor performance evaluation process. (Recommendation 8)

The NNSA Administrator should direct Information Management and the Office of Acquisition and Project Management to ensure that Supplemental Directive 205.1 contains language requiring third-party validation of contractor and subcontractor cybersecurity measures. (Recommendation 9)

Agency Comments and Our Evaluation

We provided a draft of this report to the Secretaries of Defense and Energy, and the Administrator of the National Nuclear Security Administration, for review and comment. DOD did not provide comments.

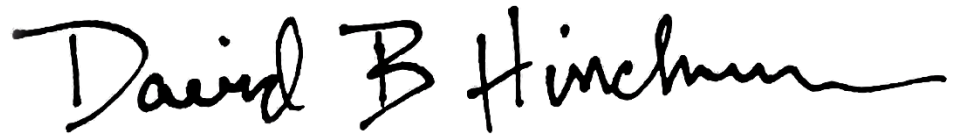
NNSA provided written comments that incorporated comments from DOE. In its comments, reproduced in appendix IX, NNSA agreed with our recommendations and described planned actions to address them. NNSA and contractor representatives from NNSA's sites also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretaries of Defense and Energy, and the Administrator of NNSA. In addition, this report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff members have any questions about this report, please contact Allison B. Bawden at (202) 512-3841 or bawdena@gao.gov, or David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made significant contributions to the report are listed in appendix X.



Allison B. Bawden
Director, Natural Resources and Environment



David B. Hinchman
Acting Director, Information Technology and Cybersecurity

List of Addressees

The Honorable Jack Reed
Chairman
The Honorable James M. Inhofe
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Dianne Feinstein
Chairwoman
The Honorable John Kennedy
Ranking Member
Subcommittee on Energy and Water Development
Committee on Appropriations
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Marcy Kaptur
Chairwoman
The Honorable Mike Simpson
Ranking Member
Subcommittee on Energy and Water Development
Committee on Appropriations
House of Representatives

The Honorable Mo Brooks
House of Representatives

The Honorable Michael Turner
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The classified annex to Senate Report 116-48 accompanying the National Defense Authorization Act for Fiscal Year 2020, includes a provision for us to review National Nuclear Security Administration's (NNSA) practices and policies for cybersecurity of nuclear weapons, and we were also asked to perform similar work. This report examines the extent to which (1) NNSA and its management and operating (M&O) contractors have implemented foundational cybersecurity risk management practices; and (2) M&O contractors oversee subcontractor cybersecurity, and NNSA efforts to enhance such oversight.

In conducting this engagement, we focused on NNSA and its seven M&O contractors that execute the agency's mission at the eight laboratory and production sites where weapons are designed, tested, and produced.¹

To examine the extent to which NNSA and its M&O contractors have implemented foundational cybersecurity risk management practices, we analyzed agency and contractor policies, procedures, strategies, and other documentation and compared them with selected practices from the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the Committee on National Security Systems (CNSS) for cybersecurity risk management. Specifically, we reviewed OMB Circular A-130: *Managing Information as a Strategic Resource*;² NIST Special Publication 800-37: *Risk Management Framework for Information Systems and Organizations*;³

¹NNSA's eight sites include the national laboratories—Lawrence Livermore in California, Los Alamos in New Mexico, and Sandia in New Mexico and California; and production sites—Y-12 National Security Complex (Y-12) in Tennessee and the Pantex Plant in Texas, the Kansas City National Security Campus (Kansas City) in Missouri, the Nevada National Security Site (Nevada Site) in Nevada, and NNSA operations at the Savannah River Site in South Carolina.

²Office of Management and Budget, *Managing Information as a Strategic Resource*, OMB Circular A-130 (Washington, D.C.: July 2016).

³National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37, Revision 2 (Gaithersburg, Md.: December 2018).

and CNSS Policy 22: Cybersecurity Risk Management.⁴ CNSS coordinates guidance relating specifically to the cybersecurity of national security systems.⁵ In addition, NIST develops specific cybersecurity standards and guidelines for federal agencies. NIST has established a risk management framework to provide a consistent and repeatable process for agencies to follow in managing their cybersecurity risk management programs and responding to cybersecurity risks.

From this review, we selected six practices identified by OMB, NIST, and CNSS that are foundational in preparing organizations to execute a risk management framework for cybersecurity. For the purpose of our review, we selected most of the foundational risk management practices that are mandatory for establishing an organization-wide risk management program, according to NIST guidance. We excluded optional organization-wide practices and all system-specific practices. Table 2 provides details on the foundational risk management practices.

Table 2. Foundational Cybersecurity Risk Management Practices for Establishing Organization-wide Cybersecurity Risk Management Programs

Category	Category description
Practice 1	Identify and assign cybersecurity risk management roles and responsibilities.
Practice 2	Establish and maintain a cybersecurity risk management strategy for the organization.
Practice 3	Document and maintain cybersecurity program policies and plans.
Practice 4	Assess and update organization-wide cybersecurity risks.

⁴Committee on National Security Systems, *Cybersecurity Risk Management Policy*, CNSS Policy 22 (Fort Meade, Md.: August 2016).

⁵For national security systems, National Security Directive 42 established CNSS, an organization chaired by the Department of Defense, to consider technical matters and develop operating policies, procedures, guidelines, instructions, and standards for national security systems. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (July 5, 1990). The Federal Information Security Modernization Act of 2014 (FISMA) defines the phrase "national security system" as any information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency where the function or operation involves intelligence activities; cryptologic activities related to national security; command and control of military forces; equipment that is an integral part of a weapon or weapons system; or, with certain exceptions, is critical to the direct fulfillment of military or intelligence missions or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy. 44 U.S.C. § 3552(6).

Appendix I: Objectives, Scope, and Methodology

Category	Category description
Practice 5	Designate controls that are available for information systems or programs to inherit.
Practice 6	Develop and maintain an organization-wide continuous monitoring strategy.

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

Further, the Department of Energy (DOE) and NNSA have established additional cybersecurity requirements through their orders (i.e., DOE Order 205.1C, *Department of Energy Cybersecurity Program*) and supplemental directives (i.e., NNSA SD 205.1, *Baseline Cybersecurity Program*, and SD 251.1B, *Directives Management*) that overlay or expound upon OMB policy, and CNSS and NIST guidance. In addition, we reviewed DOE and NNSA delegation orders, which divide and delegate responsibility for NNSA’s digital environments between the Office of Information Management (Information Management) and the Office of Defense Programs (Defense Programs). We determined that NNSA’s cybersecurity activities were broadly divided between digital environments—information technology (IT), operational and industrial technology (OT), and nuclear weapons technology (NW-IT). These practices are applicable to each of NNSA’s digital environments but should be tailored based on mission objectives and the risks of that particular environment. During our review, NNSA was developing but did not have OT or NW-IT guidance for contractors to implement a cybersecurity risk management framework. Therefore, our review focused on NNSA’s organization-level efforts and did not assess its contractors’ efforts to implement a cybersecurity risk management framework in the OT and NW-IT environments.

In evaluating NNSA and the M&O contractors’ implementation of the six foundational cybersecurity risk management practices in the IT environment, we collected and analyzed agency and site-specific cybersecurity policies and plans, organization charts, risk management and continuous monitoring strategies, risk assessment results and other cybersecurity risk-management-related documentation and compared them with the foundational risk management practices. We supplemented our analyses with interviews with relevant agency officials within Information Management and contractor representatives to discuss the development of their policies. We discussed the results of our initial analysis of agency and contractor documentation with agency officials and contractor representatives to validate our findings, collect additional evidence, and identify causes for any gaps. To gain further insight, we also interviewed officials from DOE’s Office of Enterprise Assessment

and reviewed relevant cybersecurity assessments. We then determined whether the evidence provided by the agency and its contractors addressed each foundational practice. Specifically, for each practice, we determined if the evidence provided by NNSA and its M&O contractor

1. addressed all of the practice's elements ("fully implemented"),
2. more than partially addressed the practice's elements, but not all ("substantially implemented"),
3. addressed about half of the practice's elements ("partially met"),
4. addressed some, but a minority, of the practice's elements ("minimally implemented"), or
5. did not address any of the practice's elements ("not implemented").

In evaluating NNSA's implementation of the six foundational risk management practices in the OT and NW-IT environments, we reviewed relevant documentation, such as DOE Order 205.1C; NNSA policy letters, such as the NAP 401.1, *Weapon Quality Policy*; and supplemental directives, such as SD 205.1 and SD 452.4-1, *Nuclear Enterprise Assurance*, as well as draft versions of proposed updates to some of these policies. We also reviewed additional documents supplied by Defense Programs, including the *Risk Management Guide for Defense Programs* and the *OT Assurance Guidebook*; and Defense Programs' program instructions, including business requirements, processes, and tools managed under the Defense Programs Business Process System to determine the extent to which NNSA's nascent efforts to establish OT and NW-IT cybersecurity risk management programs aligned with foundational risk management practices. We also reviewed independent assessments of NNSA's OT environment by the JASON and the Institute for Defense Analyses, and interviewed a JASON expert regarding that report's findings. To validate and corroborate our understanding of NNSA's progress in implementing the foundational risk management practices in the OT and NW-IT environments, we interviewed officials from Information Management and Defense Programs. We also interviewed officials and contractor representatives at each of the eight sites regarding cybersecurity protections at these sites. We also interviewed officials with the Department of Defense to gain their perspective on NNSA's cybersecurity measures.

To examine the extent to which NNSA and the M&O contractors oversee subcontractor cybersecurity and NNSA's plans, if any, to enhance subcontractor cybersecurity, we reviewed contractor requirements for

cybersecurity specified in the contractor requirements document sections of DOE Order 205.1C and NNSA SD 205.1, as well as draft versions of proposed updates to these documents. We also reviewed the M&O contracts for each of the seven contractors operating NNSA's eight sites to assess contractual cybersecurity requirements. On the basis of this documentation, we identified current and potential requirements for contractors to ensure that subcontractors employ cybersecurity measures. We interviewed DOE and NNSA officials, including the Office of Acquisition and Project Management, regarding NNSA's oversight of contractors and potential efforts to enhance cybersecurity oversight. We also conducted semistructured interviews with federal officials and M&O contractor representatives from the sites to determine the extent to which M&O contractors understood their cybersecurity contract requirements and were performing required oversight of subcontractors and what steps, if any, they took as part of this oversight.

We conducted this performance audit from March 2020 to September 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Details on NNSA's Implementation of Six Foundational Cybersecurity Risk Management Practices

The National Nuclear Security Administration (NNSA) fully implemented four of six foundational cybersecurity risk management practices in the traditional IT environment. However, the agency partially implemented the other two foundational risk management practices—document and maintain cybersecurity program policies and plans and develop and maintain an organization-wide continuous monitoring strategy. Table 3 provides details on our assessment.

Table 3. Extent to Which the National Nuclear Security Administration (NNSA) Implemented Six Foundational Cybersecurity Risk Management Practices

Foundational practices	Implementation status	Description
Practice 1: Identify and assign cybersecurity risk management roles and responsibilities.	fully implemented	NNSA identified and assigned individuals to specific cybersecurity risk management roles and responsibilities, such as the agency authorizing official and chief information officer. ^a Additionally, NNSA established a risk governance structure through its Enterprise Cybersecurity Advisory Board and identified the agency chief information security officer as the risk executive to guide and oversee its risk management program.
Practice 2: Establish and maintain a cybersecurity risk management strategy for the organization.	fully implemented	NNSA established a cybersecurity risk management strategy for the organization in its April 2016 Cyber Security Program Plan, which fully addressed all elements from the National Institute of Standards and Technology (NIST) guidance. ^b For instance, NNSA's plan addressed elements from NIST guidance, such as describing considerations for supply chain risks. The plan considered risks related to mission-essential functions (i.e., systems that operate in the event of a disaster) and national security systems (i.e., systems of high importance to the national security of the nation). Additionally, NNSA maintained the strategy by performing a review and making necessary updates to account for organizational changes in October 2021.

**Appendix II: Details on NNSA's Implementation
of Six Foundational Cybersecurity Risk
Management Practices**

Foundational practices	Implementation status	Description
Practice 3: Document and maintain cybersecurity program policies and plans.	partially implemented	<p>NNSA documented cybersecurity risk-based plans and policies in its April 2016 Cyber Security Program Plan and July 2017 Supplemental Directive (SD) 205.1, Baseline Cybersecurity Program. NNSA performed a review and updated its Cyber Security Program Plan in October 2021 but, as of May 2022, had not done the same for SD 205.1 within time frames specified in accordance with its directive.</p> <p>Specifically, NNSA's October 2020 SD 251.1B, Directives Management, requires that NNSA review its directives every 3 years to confirm relevancy and accuracy and further requires that documents be consistent with statutes, regulations, and other Department of Energy (DOE) and NNSA directives. However, the organization had not performed such a review of this document in nearly 5 years. Furthermore, NNSA had not updated this document to reflect new or revised NIST guidance and other changes required by DOE cybersecurity requirements.</p> <p>NNSA officials have delayed issuance of the revised directive several times—they first expected to issue it by December 2020, then successively pushed the date to June 2021, December 2021, and June 2022—and additional delays may occur if impediments continue. In May 2022, NNSA officials provided a draft version of SD 205.1, dated April 2022, but they did not have an estimated completion date for this directive.</p> <p>While NNSA has made progress to incorporate updated guidance in its directive, the draft contained gaps with respect to cybersecurity requirements. Specifically, the draft did not include specific references to two cybersecurity elements that would align it with OMB policy and Committee on National Security Systems guidance. These elements are to review and update risk management and continuous monitoring strategies within prescribed time frames. For instance, the draft version of SD 205.1 did not specify time frames for NNSA and its management and operating contractors to perform periodic reviews and updates to these strategies.</p>
Practice 4: Assess and update organization-wide cybersecurity risks.	fully implemented	<p>NNSA conducted organization-wide cybersecurity risk assessments and updated the assessment results on an ongoing basis. For instance, the agency documented the results of the assessment in its September 2020 Enterprise Assessment Report. Additionally, the agency relied on its enterprise risk register to manage cybersecurity risks across the organization.</p> <p>NNSA identified a number of organization-wide cybersecurity risks in its Enterprise Assessment Report. For instance, one risk involved ensuring that its contractors consistently follow standard operating procedures. Another risk pertained to site contractors not performing reviews and updates to risk-based documentation, in accordance with NNSA SD 205.1.</p>
Practice 5: Designate controls that are available for information systems or programs to inherit.	fully implemented	<p>NNSA identified, documented, and published an organization-wide catalog of security controls that are available for information systems or programs to inherit in its Cybersecurity Program Plan. For instance, the agency's designated security controls include monitoring network traffic data continuously to detect suspected security incidents in near real-time, reporting those incidents to federal agencies in a timely manner, and mitigating any harm to the information system.</p>

**Appendix II: Details on NNSA's Implementation
of Six Foundational Cybersecurity Risk
Management Practices**

Foundational practices	Implementation status	Description
Practice 6: Develop and maintain an organization-wide continuous monitoring strategy.	partially implemented	<p>NNSA maintained an organization-wide continuous monitoring strategy in its April 2021 Information Systems Continuous Monitoring Plan, but it did not fully develop a strategy that addressed all NIST elements.^c For instance, the strategy did not address four elements from NIST guidance, which include (1) considering supply chain risk, (2) addressing monitoring requirements across the organization, (3) defining the ongoing control assessment approach, and (4) defining security reporting requirements.</p> <p>NNSA did not include these elements for organization-wide cybersecurity risk management in its continuous monitoring strategy because it was not using the latest guidance from NIST.^d</p>

Legend: ● = fully implemented—NNSA addressed all of the practice's elements. ● = substantially implemented—NNSA more than partially addressed the practice's elements, but not all. ◐ = partially implemented—NNSA addressed about half of the practice's elements. ◑ = minimally implemented—NNSA addressed some, but a minority, of the practice's elements. ○ = not implemented—NNSA did not address any of the practice's elements.

Source: GAO analysis of agency data. | GAO-22-104195

^aAccording to NIST SP 800-37, Revision 2, key participants in risk management processes include (1) the head of agency, (2) the authorizing official or authorizing official designated representative, (3) the chief information officer, (4) the senior accountable official for risk management or risk executive function, and (5) senior agency information security officer.

^bAccording to NIST SP 800-37, Revision 2, a risk management strategy should include several elements. These elements include (1) expressing organizational risk tolerance; (2) guiding and informing risk-based decisions that describe how security risk is framed, assessed, responded to, and monitored; (3) determining risk assessment methodologies; (4) determining risk response strategies; (5) defining a process for consistently evaluating security risks organization-wide; (6) describing considerations for supply chain risk; (7) defining approaches for monitoring risk over time; (8) defining strategic-level decisions and considerations for how senior leaders and executives are to manage cybersecurity risks to organizational operations, organizational assets, individuals, other organizations, and the nation; and (9) including an explicit statement of the threats, assumptions, constraints, priorities, trade-offs, and risk tolerance used for making investment and operational decisions.

^cAccording to NIST SP 800-37, Revision 2, a continuous monitoring strategy should include several elements. These elements include (1) considering supply chain risk, (2) addressing monitoring requirements across the organization, (3) identifying the minimum monitoring frequency for implemented security controls across the organization, (4) defining the ongoing control assessment approach, (5) describing how ongoing assessments are to be conducted, (6) defining security reporting requirements and recipients of the reports, and (7) authorizing the strategy for approval by the senior accountable official for risk management or the risk executive (function).

^dIn December 2018, NIST revised its risk management framework to include additional steps for organizations in preparing for risk management.

Appendix III: Details on NNSA Contractors' Identification and Assignment of Risk Management Roles and Responsibilities

Two of the seven management and operating (M&O) contractors—Pantex/Y-12 and Savannah River—in our review fully implemented elements of a foundational cybersecurity risk management practice: Identify and assign cybersecurity risk management roles and responsibilities at National Nuclear Security Administration's (NNSA) eight national laboratory and production sites in the traditional IT environment.¹ Four contractors—Lawrence Livermore, Los Alamos, Nevada Site, and Sandia—substantially implemented this foundational practice, while one contractor—Kansas City—partially implemented this practice. Each M&O contractor established a risk governance structure through site councils, such as the Site Risk Management Council, consistent with NNSA's supplemental directive on cybersecurity. Table 4 provides details on our assessment.

Table 4: Extent to Which the National Nuclear Security Administration's (NNSA) Management and Operating (M&O) Contractors Identified and Assigned Cybersecurity Risk Management Roles and Responsibilities

NNSA site	Implementation status	Description
Kansas City National Security Campus	partially implemented	The M&O contractor established a site-wide risk governance structure through its Active Risk Matrix Council, but it only partially identified and assigned individuals to specific cybersecurity risk management roles and responsibilities. For instance, the contractor's Cyber Security Program Plan and Site Specific Risk Management Plan did not identify four key roles and responsibilities. These four key roles were the site's authorizing official designated representative, risk executive, chief information officer, and senior accountable official for risk management. Furthermore, the contractor did not assign a key role to a specific individual or group—senior accountable official for risk management—to guide and oversee its risk management program.

¹According to NIST SP 800-37, Revision 2, key participants in risk management processes include (1) the head of agency, (2) the authorizing official or authorizing official designated representative, (3) the chief information officer, (4) the senior accountable official for risk management or risk executive function, and (5) the senior agency information security officer.

**Appendix III: Details on NNSA Contractors'
Identification and Assignment of Risk
Management Roles and Responsibilities**

NNSA site	Implementation status	Description
Lawrence Livermore National Laboratory	substantially implemented	<p>The M&O contractor identified and assigned specific individuals to cybersecurity risk management roles and responsibilities, such as the site's chief information officer. Additionally, the contractor established a risk governance structure through its Site Risk Management Council and the site chief information officer as the risk executive to guide and oversee the contractor's risk management program.</p> <p>An individual serves as the site's authorizing official designated representative, according to its point of contact list, but the contractor did not identify this individual's roles and responsibilities in its Cyber Security Program Plan, which is inconsistent with National Institute of Standards and Technology (NIST) guidance.</p>
Los Alamos National Laboratory	substantially implemented	<p>The M&O contractor identified and assigned specific individuals to cybersecurity risk management roles and responsibilities, such as the senior information security manager. Additionally, the contractor established a risk governance structure through its Site Risk Management Council and the Information Systems and Cybersecurity Performance Assurance Council as the risk executive to guide and oversee the contractor's risk management program.</p> <p>However, the contractor did not identify roles and responsibilities for the authorizing official designated representative in its Cyber Security Program Plan.</p>
Nevada National Security Site	substantially implemented	<p>The M&O contractor identified and assigned individuals to specific cybersecurity risk management roles and responsibilities, such as the site's senior agency information security officer. Additionally, the contractor established a risk governance structure through its Risks and Issues Board and the Risk Review Board as the risk executive to guide and oversee contractor's risk management program.</p> <p>However, inconsistent with NIST guidance, the contractor did not identify the authorizing official designated representative's roles and responsibilities in its Cyber Security Program Plan. As of May 2022, NNSA had not assigned a specific individual to this role at the Nevada National Security Site.</p>
Pantex Plant and Y-12 National Security Complex ^a	fully implemented	<p>The M&O contractor identified and assigned individuals to specific cybersecurity risk management roles and responsibilities, such as the site's chief information officer. Additionally, the contractor established a risk governance structure through its Site Risk Management Council and the site chief information officer as the risk executive to guide and oversee contractor's risk management program.</p>
Sandia National Laboratories	substantially implemented	<p>The M&O contractor identified and assigned specific individuals to cybersecurity risk management roles and responsibilities, such as the site's senior information security manager. Additionally, the contractor established a risk governance structure through its Site Risk Management Council and the senior information security manager as the risk executive to guide and oversee the contractor's risk management program.</p> <p>An individual serves as the site's current authorizing official designated representative, according to system inventory reports, but the contractor did not identify this individual's roles and responsibilities in its Cyber Security Program Plan.</p>

**Appendix III: Details on NNSA Contractors'
Identification and Assignment of Risk
Management Roles and Responsibilities**

NNSA site	Implementation status	Description
Savannah River Site (NNSA operations)	fully implemented	The M&O contractor identified and assigned specific individuals to cybersecurity risk management roles and responsibilities, such as the site's senior information security manager. Additionally, the contractor established a risk governance structure through its Chief Information Officers Council and the Department of Energy's Office of Environmental Management authorizing official as the risk executive to guide and oversee the contractor's risk management program. As of February 2022, NNSA had not assigned an individual to serve in the role of authorizing official designated representative at the Savannah River Field Office but had plans to do so by October 2022.

Legend: ● = fully implemented—M&O contractor addressed all of the practice's elements. ● = substantially implemented—M&O contractor more than partially addressed the practice's elements, but not all. ◐ = partially implemented—M&O contractor addressed about half of the practice's elements. ◑ = minimally implemented—M&O contractor addressed some, but a minority, of the practice's elements. ○ = not implemented—M&O contractor did not address any of the practice's elements.

Source: GAO analysis of contractor data. | GAO-22-104195

Note: NNSA's M&O contractors are to follow six foundational practices for organization-wide cybersecurity risk management, including identifying and assigning cybersecurity risk management roles and responsibilities.

^aThe Pantex Plant and Y-12 National Security Complex are separate sites managed and operated by a common contractor under a common contract.

Appendix IV: Details on NNSA Contractors' Establishment and Maintenance of Cybersecurity Risk Management Strategies

Four of the seven National Nuclear Security Administration (NNSA) management and operating (M&O) contractors—Kansas City, Lawrence Livermore, the Nevada Site, and Pantex/Y-12—in our review fully implemented elements of a foundational cybersecurity risk management practice: Establish and maintain cybersecurity risk management strategies at NNSA's eight national laboratory and production sites in the traditional IT environment.¹ Two contractors—Los Alamos and Sandia—substantially implemented this practice, and one—the contractor managing NNSA operations at Savannah River—partially implemented this practice. For instance, six of the M&O contractors maintained strategies to account for organizational changes, but the contractor at Savannah River had not done so. Table 5 provides details on our assessment.

¹According to NIST SP 800-37, Revision 2, a risk management strategy should include several elements. These elements include (1) expressing organizational risk tolerance; (2) guiding and informing risk-based decisions that describe how security risk is framed assessed, responded to, and monitored; (3) determining risk assessment methodologies; (4) determining risk response strategies; (5) defining a process for consistently evaluating security risks organization-wide; (6) describing considerations for supply chain risk; (7) defining approaches for monitoring risk over time; (8) defining strategic-level decisions and considerations for how senior leaders and executives are to manage cybersecurity risks to organizational operations, organizational assets, individuals, other organizations, and the nation; and (9) including an explicit statement of the threats, assumptions, constraints, priorities, trade-offs, and risk tolerance used for making investment and operational decisions.

Appendix IV: Details on NNSA Contractors' Establishment and Maintenance of Cybersecurity Risk Management Strategies

Table 5: Extent to Which the National Nuclear Security Administration's (NNSA) Management and Operating (M&O) Contractors Established and Maintained Cybersecurity Risk Management Strategies

NNSA site	Implementation status	Description
Kansas City National Security Campus	fully implemented	<p>The M&O contractor established and maintained a site-wide risk management strategy in its September 2019 Site Specific Risk Management Plan. This strategy addressed all elements from the National Institute of Standards and Technology (NIST) guidance, such as determining the methodology for conducting a risk assessment and a strategy for responding to cybersecurity risk.</p> <p>Additionally, through its strategy, the contractor communicated site-wide cybersecurity threats, vulnerabilities, and risk-related information to NNSA leadership through weekly site-specific risk management meetings to help inform risk-based decisions. The contractor also provided a site-wide view for managing cybersecurity risk throughout the organization through its risk governance process (i.e., a risk management activity that delegates roles and responsibilities to key stakeholders throughout the organization).</p>
Lawrence Livermore National Laboratory	fully implemented	<p>The M&O contractor established and maintained a site-wide risk management strategy in its risk-based documents, such as the January 2020 Cybersecurity Program Plan. This strategy addressed all elements from the NIST guidance, such as describing considerations for supply chain risk and defining approaches for monitoring risk over time.</p> <p>Additionally, through its strategy, the contractor communicated site-wide cybersecurity threats, vulnerabilities, and risk-related information to NNSA leadership via an automated reporting tool to help inform risk-based decisions. The contractor also provided a site-wide view for managing cybersecurity risk throughout the organization through its risk governance process.</p>
Los Alamos National Laboratory	substantially implemented	<p>As part of the M&O contractor's risk management processes, it communicated site-wide cybersecurity threat, vulnerability, and risk-related information to NNSA leadership via an automated reporting tool to help inform risk-based decisions. The contractor also provided a strategic view for managing cybersecurity risk throughout the organization through its risk governance process.</p> <p>Additionally, the M&O contractor established and maintained a site-wide risk management strategy in its August 2019 Cybersecurity Program Plan. This strategy addressed most of the elements from the NIST guidance, such as describing considerations for supply chain risk and defining approaches for monitoring risk over time.</p> <p>However, the strategy did not fully address two elements from the NIST guidance—risk assessment methodologies and risk response strategy.</p>

Appendix IV: Details on NNSA Contractors' Establishment and Maintenance of Cybersecurity Risk Management Strategies

NNSA site	Implementation status	Description
Nevada National Security Site	fully implemented	<p>The M&O contractor established and maintained a site-wide risk management strategy in its January 2019 Risk Management company directive. This strategy addressed all elements from the NIST guidance, such as risk assessment methodologies and risk response strategy.</p> <p>Additionally, through its strategy, the contractor communicated site-wide cybersecurity threats, vulnerabilities, and risk-related information to NNSA leadership via an automated reporting tool to help inform risk-based decisions. The contractor also provided a site-wide view for managing cybersecurity risk throughout the organization through its risk disposition process (i.e., a risk management activity that involves senior executives and stakeholders who deliberate and determine the appropriate risk response action to take for mitigating cybersecurity risks).</p>
Pantex Plant and Y-12 National Security Complex ^a	fully implemented	<p>The M&O contractor established and maintained a site-wide risk management strategy in its risk-based documents—which consists of the February 2018 Enterprise Risk Management Process, August 2019 Cyber Security Threat Statement, and August 2019 Cybersecurity Program Plan. This strategy addressed all of the elements from NIST guidance, such as guiding and informing risk-based decisions, describing considerations for supply chain risk, and defining an approach for monitoring risk over time.</p> <p>Additionally, as called for by its strategy, the contractor communicated site-wide cybersecurity threat, vulnerability, and risk-related information to NNSA leadership via automated reporting tools to help inform risk-based decisions. The contractor's strategy also provided a strategic view for managing cybersecurity risk throughout the organization through the contractor's risk governance process.</p>
Sandia National Laboratories	substantially implemented	<p>As part of the M&O contractor's risk management processes, it communicated site-wide cybersecurity threat, vulnerability, and risk-related information to NNSA leadership via automated reporting tools to help inform risk-based decisions. The strategy also provided a strategic view for managing cybersecurity risk throughout the organization through its risk governance process.</p> <p>Additionally, the M&O contractor established and maintained a site-wide risk management strategy in its December 2017 Information Security Risk Management Plan. This strategy addressed most of the elements from the NIST guidance, such as guiding and informing risk-based decisions, describing considerations for supply chain risk, and defining an approach for monitoring risk over time.</p> <p>However, the strategy did not fully address one element—determining risk assessment methodologies. Aspects of a risk assessment methodology that were not addressed include (1) providing a high-level overview of the risk assessment process, (2) describing the assessment approach (e.g., quantitative, qualitative, or semiquantitative), and (3) providing an analysis approach (i.e., threat-oriented, asset/impact-oriented, vulnerability-oriented).</p>

Appendix IV: Details on NNSA Contractors' Establishment and Maintenance of Cybersecurity Risk Management Strategies

NNSA site	Implementation status	Description
Savannah River Site (NNSA operations)	partially implemented	<p>As part of the M&O contractor's risk management processes, it communicated site-wide cybersecurity threat, vulnerability, and risk-related information to NNSA leadership via reporting tools to help inform risk-based decisions. The contractor also provided a strategic view for managing cybersecurity risk throughout the organization through its risk governance process.</p> <p>Additionally, the M&O contractor established a site-wide risk management strategy in its October 2016 Savannah River Risk and Opportunity Management Plan. This strategy addressed all elements from the NIST guidance, such as describing considerations for supply chain risk and defining an approach for monitoring risk over time.</p> <p>However, inconsistent with NIST and Committee on National Security Systems guidance, this contractor had not performed an annual review of its strategy and updated it accordingly to account for organizational changes to its site for over 5 years. In March 2022, contractor representatives stated that the contractor planned to review and update Savannah River Risk and Opportunity Management Plan later in calendar year 2022. Subsequently, in May, the contractor provided supplemental evidence—March 2022 Operational Risk and Opportunity Report—that they believe addressed this deficiency. However, this report focused on an assessment of site-wide cybersecurity risk and did not reflect the contractor's review of its risk management strategy.</p>

Legend: ● = fully implemented—M&O contractor addressed all of the practice's elements. ● = substantially implemented—M&O contractor more than partially addressed the practice's elements, but not all. ◐ = partially implemented—M&O contractor addressed about half of the practice's elements. ◑ = minimally implemented—M&O contractor addressed some, but a minority, of the practice's elements. ○ = not implemented—M&O contractor did not address any of the practice's elements.

Source: GAO analysis of contractor data. | GAO-22-104195

Note: NNSA's M&O contractors are to follow six foundational practices for organization-wide cybersecurity risk management, including establishing and maintaining cybersecurity risk management strategies.

^aThe Pantex Plant and Y-12 National Security Complex are separate sites managed and operated by a common contractor under a common contract.

Appendix V: Details on NNSA Contractors’ Documentation and Maintenance of Cybersecurity Program Policies

All seven of the management and operating (M&O) contractors in our review fully implemented elements of a foundational cybersecurity risk management practice: Document and maintain cybersecurity program policies and plans at National Nuclear Security Administration’s (NNSA) eight national laboratory and production sites in the traditional IT environment. Each M&O contractor maintained their respective site-wide cybersecurity program plans. Table 6 provides details on our assessment.

Table 6: Extent to Which the National Nuclear Security Administration’s (NNSA) Management and Operating (M&O) Contractors Documented and Maintained Cybersecurity Program Policies and Plans

NNSA site	Implementation status	Description
Kansas City National Security Campus	fully implemented	The M&O contractor documented and maintained a site-wide cybersecurity program policy and plan. For instance, the contractor updated its Cyber Security Policy in October 2019 to account for organizational changes, such as realigning the policy to the National Institute of Standards and Technology Special Publication 800-53 and the Committee on National Security Systems Instruction 1253.
Lawrence Livermore National Laboratory	fully implemented	The M&O contractor documented and maintained a site-wide cybersecurity program policy and plan. For instance, the contractor updated its Cyber Security Program Plan in January 2020 for information systems to account for organizational changes.
Los Alamos National Laboratory	fully implemented	The M&O contractor documented and maintained a site-wide cybersecurity program policy and plan. For instance, the contractor updated its Cybersecurity Program Plan in August 2019 to account for organizational changes.
Nevada National Security Site	fully implemented	The M&O contractor documented and maintained a site-wide cybersecurity program policy and plan. For instance, the contractor updated its Cyber Security Risk Management policy in March 2019 to account for organizational changes.
Pantex Plant and Y-12 National Security Complex ^a	fully implemented	The M&O contractor for both sites documented a site-wide cybersecurity program policy— <i>Consolidated Nuclear Security Enterprise Common Policies and Procedures</i> —and plan— <i>Consolidated Nuclear Security Cyber Security Program Plan</i> . The contractor also updated its policy and plan in July 2019 and August 2019, respectively, to account for organizational changes.

**Appendix V: Details on NNSA Contractors'
Documentation and Maintenance of
Cybersecurity Program Policies**

NNSA site	Implementation status	Description
Sandia National Laboratories	fully implemented	The M&O contractor documented and maintained a site-wide cybersecurity program policy and plan. For instance, the contractor documented its plan in two separate cybersecurity program plans, dated December 2017 and July 2018, for its computing environments.
Savannah River Site (NNSA operations)	fully implemented	The M&O contractor documented and maintained a site-wide cybersecurity program policy and plan. For instance, the contractor updated its cybersecurity program plan in January 2019 to account for organizational changes.

Legend: ● = fully implemented—M&O contractor addressed all of the practice’s elements. ● = substantially implemented—M&O contractor more than partially addressed the practice’s elements, but not all. ◐ = partially implemented—M&O contractor addressed about half of the practice’s elements. ◑ = minimally implemented—M&O contractor addressed some, but a minority, of the practice’s elements. ○ = not implemented—M&O contractor did not address any of the practice’s elements.

Source: GAO analysis of contractor data. | GAO-22-104195

Note: NNSA’s M&O contractors are to follow six foundational practices for organization-wide cybersecurity risk management, including documenting and maintaining cybersecurity program policies and plans.

^aThe Pantex Plant and Y-12 National Security Complex are separate sites managed and operated by a common contractor under a common contract.

Appendix VI: Details on NNSA Contractors' Assessment and Update of Organizational Cybersecurity Risks

All seven of the management and operating (M&O) contractors in our review fully implemented elements of a foundational cybersecurity risk management practice: Assess and update organization-wide cybersecurity risks at National Nuclear Security Administration's (NNSA) eight national laboratory and production sites in the traditional IT environment. Each M&O contractor documented the results of its risk assessments in various sources, such as site-wide risk assessment reports and individual improvement plans. Table 7 provides details on our assessment.

Table 7: Extent to Which the National Nuclear Security Administration's (NNSA) Management and Operating (M&O) Contractors Assessed and Updated Cybersecurity Risks

NNSA site	Implementation status	Description
Kansas City National Security Campus	fully implemented	<p>The M&O contractor conducted site-wide cybersecurity risk assessments and updated the assessment results on an ongoing basis. For instance, the contractor documented the results of the assessment in its July 2020 Site Improvement Plan.</p> <p>According to the contractor's October 2020 self-assessment report, the top site-wide risks include reporting security incidents within required timeframes and adhering to supply chain risk management processes.</p>
Lawrence Livermore National Laboratory	fully implemented	<p>The M&O contractor conducted site-wide cybersecurity risk assessments and updated the assessment results on an ongoing basis. For instance, the contractor documented the results of the assessment in its April 2020 risk assessment report.</p> <p>NNSA's July 2020 risk register included several of the contractor's top site-wide cybersecurity risks. These cyber risks include maintaining network segmentation and funding end-of-life computing resources (i.e., information systems and components not supportable by a developer, vendor, or manufacturer).</p>

Appendix VI: Details on NNSA Contractors' Assessment and Update of Organizational Cybersecurity Risks

NNSA site	Implementation status	Description
Los Alamos National Laboratory	fully implemented	<p>The M&O contractor conducted site-wide cybersecurity risk assessments and updated the assessment results on an ongoing basis. For instance, the contractor documented the results of the assessment in its July 2020 cybersecurity improvement plan.</p> <p>According to the plan, the top site-wide cybersecurity risks include performing periodic vulnerability scans on computing resources, and applying consistent baseline configuration settings (i.e., a documented set of specifications for an information system).</p>
Nevada National Security Site	fully implemented	<p>The M&O contractor conducted site-wide cybersecurity risk assessments and updated the assessment results on an ongoing basis. For instance, the contractor documented the results of the assessment in its July 2020 cybersecurity improvement plan.</p> <p>According to the plan, the top site-wide cybersecurity risks include multi-factor authentication (i.e., the means used to confirm the identity of a user, process, or device) and network segmentation.</p>
Pantex Plant and Y-12 National Security Complex ^a	fully implemented	<p>The M&O contractor conducted site-wide cybersecurity risk assessments and updated the assessment results on an ongoing basis. For instance, the contractor documented the results of the assessment in its August 2019 cybersecurity improvement plan.</p> <p>According to its December 2020 <i>Cyber Security Risk Summary</i> report, the top site-wide cybersecurity risks include recruiting and retaining skilled cyber workforce and improving incident response capabilities.</p>
Sandia National Laboratories	fully implemented	<p>The M&O contractor conducted site-wide cybersecurity risk assessments and updated the assessment results on an ongoing basis. For instance, the contractor conducted two site-wide risk assessments of its computing environments in January and December 2020.</p> <p>According to the cyber risk assessment reports, the top site-wide cybersecurity risks include active insider threats, natural and environmental disasters, and advanced persistent threats (i.e., an adversary possessing sophisticated levels of expertise and significant resources to pursue its goal of continuously impeding critical aspects of an organization's mission objectives to repeatedly exfiltrate information over an extended period of time).</p>
Savannah River Site (NNSA operations)	fully implemented	<p>The M&O contractor conducted site-wide cybersecurity risk assessments and updated the assessment results on an ongoing basis. For instance, the contractor documented the results of the assessment in its cybersecurity improvement plan.</p> <p>According to the contractor's April 2019 plan, the top risks include implementing methods to detect the unauthorized transfer of information from an information system and ensuring that appropriate personnel receive information spillage response training.</p>

Legend: ● = fully implemented—M&O contractor addressed all of the practice's elements. ● = substantially implemented—M&O contractor more than partially addressed the practice's elements, but not all. ◐ = partially implemented—M&O contractor addressed about half of the practice's elements. ◑ = minimally implemented—M&O contractor addressed some, but a minority, of the practice's elements. ○ = not implemented—M&O contractor did not address any of the practice's elements.

Source: GAO analysis of contractor data. | GAO-22-104195

Note: NNSA's M&O contractors are to follow six foundational practices for organization-wide cybersecurity risk management, including assessing and updating organization-wide cybersecurity risks.

**Appendix VI: Details on NNSA Contractors'
Assessment and Update of Organizational
Cybersecurity Risks**

^aThe Pantex Plant and Y-12 National Security Complex are separate sites managed and operated by a common contractor under a common contract.

Appendix VII: Details on NNSA Contractors' Designation of Controls Available for Inheritance

All seven of the management and operating (M&O) contractors in our review fully implemented elements of a foundational cybersecurity risk management practice: Designate controls that are available for information systems or programs to inherit at National Nuclear Security Administration's eight national laboratory and production sites in the traditional IT environment. Each M&O contractor designated controls (e.g., security awareness training, security assessments, and incident handling, etc.) in various sources, such as site-wide cybersecurity program plans and policies, common control catalogs, and individual system security plans. Table 8 provides details on our assessment.

Table 8: Extent to Which the National Nuclear Security Administration's (NNSA) Management and Operating (M&O) Contractors Designated Controls Available for Inheritance by Information Systems or Programs

NNSA site	Implementation status	Description
Kansas City National Security Campus	fully implemented	The M&O contractor identified, documented, and published a catalog of security controls that are available for information systems or programs to inherit in its Cyber Security Policy. For instance, inherited security controls include security assessment, information sharing, and security awareness training.
Lawrence Livermore National Laboratory	fully implemented	The M&O contractor identified, documented, and published a catalog of security controls that are available for information systems or programs to inherit in its Common Controls Catalog. For instance, inherited security controls include security awareness training and baseline configuration (i.e., a documented set of specifications for an information system).
Los Alamos National Laboratory	fully implemented	The M&O contractor identified, documented, and published a catalog of security controls that are available for information systems or programs to inherit in its individual security plans. For instance, inherited security controls include contingency plans, security assessments, and least functionality (i.e., users and programs should only have the necessary privileges to complete their tasks).
Nevada National Security Site	fully implemented	The M&O contractor identified, documented, and published a catalog of security controls that are available for information systems or programs to inherit in its common controls catalog. For instance, inherited security controls include account management, incident reporting, and separation of duties (i.e., no user should be given enough privileges to misuse the system on their own).

**Appendix VII: Details on NNSA Contractors’
Designation of Controls Available for
Inheritance**

NNSA site	Implementation status	Description
Pantex Plant and Y-12 National Security Complex ^a	fully implemented	The M&O contractor identified, documented, and published a catalog of security controls that are available for information systems or programs to inherit in its cybersecurity program plan. For instance, inherited security controls include security assessment, continuous monitoring, and vulnerability scanning.
Sandia National Laboratories	fully implemented	The M&O contractor identified, documented, and published a catalog of security controls that are available for information systems or programs to inherit in its enterprise control libraries. For instance, inherited security controls include security awareness training, security assessment, and incident handling (i.e., mitigation of violations of security policies and recommended practices).
Savannah River Site (NNSA operations)	fully implemented	The M&O contractor identified, documented, and published a catalog of security controls that are available for information systems or programs to inherit in its cybersecurity program plan. For instance, inherited security controls include supply chain protection, continuous monitoring, and risk assessment.

Legend: ● = fully implemented—M&O contractor addressed all of the practice’s elements. ● = substantially implemented—M&O contractor more than partially addressed the practice’s elements, but not all. ◐ = partially implemented—M&O contractor addressed about half of the practice’s elements. ◑ = minimally implemented—M&O contractor addressed some, but a minority, of the practice’s elements. ○ = not implemented—M&O contractor did not address any of the practice’s elements.

Source: GAO analysis of contractor data. | GAO-22-104195

Note: NNSA’s M&O contractors are to follow six foundational practices for organization-wide cybersecurity risk management, including designating controls that are available for information systems or programs to inherit.

^aThe Pantex Plant and Y-12 National Security Complex are separate sites managed and operated by a common contractor under a common contract.

Appendix VIII: Details on NNSA Contractors' Development and Maintenance of Continuous Monitoring Strategies

Four of the seven National Nuclear Security Administration (NNSA) management and operating (M&O) contractors—Lawrence Livermore, Los Alamos, Pantex/Y-12, and Sandia—in our review substantially implemented elements of a foundational cybersecurity risk management practice: Develop and maintain organization-wide continuous monitoring strategies at NNSA's eight national laboratory and production sites in the traditional IT environment. One contractor at Savannah River partially implemented the foundational practice, while two others—Kansas City and the Nevada Site—minimally implemented this practice. Furthermore, we found that no contractor's strategy fully addressed all elements from National Institute of Standards and Technology (NIST) guidance.¹ Table 9 provides details on our assessment.

¹According to NIST SP 800-37, Revision 2, a continuous monitoring strategy should include several elements. These elements include (1) considering supply chain risk, (2) addressing monitoring requirements across the organization, (3) identifying the minimum monitoring frequency for implemented security controls across the organization, (4) defining the ongoing control assessment approach, (5) describing how ongoing assessments are to be conducted, (6) defining security reporting requirements and recipients of the reports, and (7) authorizing the strategy for approval by the senior accountable official for risk management or the risk executive (function).

**Appendix VIII: Details on NNSA Contractors’
Development and Maintenance of Continuous
Monitoring Strategies**

Table 9: Extent to Which the National Nuclear Security Administration’s (NNSA) Management and Operating (M&O) Contractors Developed and Maintained Cybersecurity Continuous Monitoring Strategies

NNSA site	Implementation status	Description
Kansas City National Security Campus	minimally implemented	<p>The M&O contractor had minimally developed and maintained a site-wide continuous monitoring strategy. Contractor representatives provided its September 2019 Site Specific Risk Management Plan, as well as documentation related to executing continuous monitoring activities, such as continuous monitoring status reports and metrics data. Contractor representatives believed that, taken together, this documentation constituted a continuous monitoring strategy.</p> <p>However, this documentation was not consistent with the continuous monitoring practice in a number of ways. The documentation provided by representatives addressed one element of a continuous monitoring strategy from National Institute of Standards and Technology (NIST) guidance—addressing monitoring requirements across the organization. At the same time, the contractor documentation did not address other elements, such as defining security reporting requirements and identifying the minimum monitoring frequencies for implemented security controls across the organization. In addition, the execution of continuous monitoring activities does not replace the need for a strategy that defines the activities that should occur, ongoing assessment approaches, and the frequency of monitoring. Contractor representatives stated that the contractor expects to complete development of a strategy by September 2022.</p>
Lawrence Livermore National Laboratory	substantially implemented	<p>The M&O contractor developed and maintained a site-wide continuous monitoring strategy in its June 2020 Information Security Continuous Monitoring Strategy and Implementation. This strategy addressed most of the elements from NIST guidance, such as defining security reporting requirements and minimum monitoring frequencies. However, the strategy did not fully address two elements—describing considerations for supply chain risk and addressing monitoring requirements across the organization.</p> <p>Contractor representatives stated that its company policies and other risk-based documentation related to supply chain risk, vulnerability, patch, and configuration management addressed these two missing elements. The contractor’s procurement procedure and July 2018 Patch and Vulnerability Management Implementation Manual addressed these elements but did not address these elements in its continuous monitoring strategy as recommended by NIST. In March 2022, contractor representatives planned to revise its existing strategy this calendar year to reflect the two missing elements from NIST guidance and stated that they created a corrective action plan to track the status of the update.</p>
Los Alamos National Laboratory	substantially implemented	<p>The M&O contractor developed and maintained a site-wide continuous monitoring strategy in its June 2021 Information System Continuous Monitoring and Ongoing Authorization Implementation Plan. This strategy addressed most of the elements from NIST guidance, such as defining security reporting requirements and minimum monitoring frequencies. However, the strategy did not fully address one element—describing how ongoing risk assessments are to be conducted. For instance, the strategy did not describe instructions for conducting an ongoing assessment of security controls for which monitoring cannot be automated using technical tools.</p>

**Appendix VIII: Details on NNSA Contractors’
Development and Maintenance of Continuous
Monitoring Strategies**

NNSA site	Implementation status	Description
Nevada National Security Site	minimally implemented	<p>The M&O contractor had minimally developed and maintained a site-wide continuous monitoring strategy. Contractor representatives provided its August 2019 Continuous Monitoring Policy, as well as documentation related to executing continuous monitoring activities, such as continuous monitoring status reports and metrics data. Contractor representatives told us they believed that, taken together, this documentation constituted a continuous monitoring strategy.</p> <p>However, this documentation was not consistent with the continuous monitoring practice in a number of ways. The documentation provided by representatives addressed one element of a continuous monitoring strategy from NIST guidance—addressing monitoring requirements across the organization. At the same time, the contractor documentation did not address other elements, such as defining security reporting requirements and identifying the minimum monitoring frequencies for implemented security controls across the organization. In addition, the execution of continuous monitoring activities does not replace the need for a strategy that defines the activities that should occur, ongoing assessment approaches, and the frequency of monitoring.</p> <p>Contractor representatives at the Nevada Site initially had no plans to develop a strategy and would continue to rely on existing documentation. However, after reviewing a draft of our report, contractor representatives stated that they had decided to change their approach and that they would develop a documented continuous monitoring plan to address all elements of the NIST guidance.</p>
Pantex Plant and Y-12 National Security Complex ^a	substantially implemented	<p>The M&O contractor developed and maintained a site-wide continuous monitoring strategy in its September 2020 Information Security Continuous Monitoring Implementation Plan. This strategy addressed most of the elements from NIST guidance, such as addressing monitoring requirements and identifying the minimum monitoring frequencies. However, the strategy did not address one element—considering supply chain risk. The contractor’s April 2018 Foreign Ownership, Control, or Influence and Subcontractor Registration procedure addressed this element but did not address this element in its continuous monitoring strategy, as recommended by NIST.</p>
Sandia National Laboratories	substantially implemented	<p>The M&O contractor developed and maintained a site-wide continuous monitoring strategy in its September 2019 Information Security Continuous Monitoring Plan. This strategy addressed most of the elements from NIST guidance, such as security reporting requirements and minimum monitoring frequencies. However, the strategy did not fully address one element—considering supply chain risk. The contractor’s procurement policies addressed this element. However, the contractor did not address this element in its continuous monitoring strategy, as recommended by NIST.</p>

**Appendix VIII: Details on NNSA Contractors'
Development and Maintenance of Continuous
Monitoring Strategies**

NNSA site	Implementation status	Description
Savannah River Site (NNSA operations)	partially implemented	<p>The M&O contractor developed a site-wide continuous monitoring strategy in its March 2020 Continuous Monitoring Plan for the NNSA Savannah River Field Office Authorization Boundaries that addressed most of the elements from the NIST guidance, such as defining security reporting requirements and identifying minimum monitoring frequencies.</p> <p>However, the contractor's strategy did not address two elements from NIST guidance—considering supply chain risk and describing how ongoing risk assessments are to be conducted—in its strategy. Specifically, the contractor's requisition security review process (i.e., activities that involve stakeholder coordination aimed at developing and integrating supply chain risk management tools into the site's procurement process) addressed the first missing element—considering supply chain risk. However, the contractor did not address this element in its continuous monitoring strategy, as recommended by NIST. The contractor did not provide evidence that addressed the second missing element—describing how ongoing risk assessments are to be conducted. In May 2022, representatives stated that, once modifications to its contract are completed, they planned to revise the strategy to be consistent with NIST guidance.</p> <p>Further, the contractor had not maintained the strategy to address cybersecurity risks and requirements across the organization. Specifically, the contractor had not updated its strategy in over 2 years. In March 2022, contractor representatives stated that the strategy is undergoing review and updates, with a planned completion date by September 2022.</p>

Legend: ● = fully implemented—M&O contractor addressed all of the practice's elements. ● = substantially implemented—M&O contractor more than partially addressed the practice's elements, but not all. ● = partially implemented—M&O contractor addressed about half of the practice's elements. ○ = minimally implemented—M&O contractor addressed some, but a minority, of the practice's elements. ○ = not implemented—M&O contractor did not address any of the practice's elements.

Source: GAO analysis of contractor data. | GAO-22-104195

Note: NNSA's M&O contractors are to follow six foundational practices for organization-wide cybersecurity risk management, including developing and maintaining organization-wide continuous monitoring strategies.

^aThe Pantex Plant and Y-12 National Security Complex are separate sites managed and operated by a common contractor under a common contract.

Appendix IX: Comments from the National Nuclear Security Administration

**Appendix IX: Comments from the National
Nuclear Security Administration**



Department of Energy
Under Secretary for Nuclear Security
Administrator, National Nuclear Security Administration
Washington, DC 20585



September 2, 2022

Ms. Allison B. Bawden
Director, Natural Resources
and Environment
U.S. Government Accountability Office
Washington, DC 20548

Dear Ms. Bawden:

Thank you for the opportunity to review the Government Accountability Office (GAO) draft report "Nuclear Weapons Cybersecurity: NNSA Should Fully Implement Foundational Cybersecurity Risk Management Practices" (GAO-22-104195). The Department of Energy's National Nuclear Security Administration (DOE/NNSA) recognizes the importance of cybersecurity, including nuclear weapon cybersecurity and for the associated equipment used for production and testing. As noted in the report, DOE/NNSA has taken positive steps to address the ever-growing digital threat to our programs.

DOE/NNSA appreciates GAO's observations on our efforts so far, and we welcome the auditors' recommendations for further enhancing our cybersecurity risk management practices. The attached Management Decision outlines the specific actions planned to address each recommendation. Our subject matter experts have also provided technical and general comments under separate cover for your consideration to enhance the clarity and accuracy of the report. If you have any questions about this response, please contact Dean Childs, Director, Audits and Internal Affairs, at (202) 836-3327.

Sincerely,

A handwritten signature in blue ink that reads "Jill Hruby".

Jill Hruby

Enclosure

Enclosure

NATIONAL NUCLEAR SECURITY ADMINISTRATION
Management Decision

**"Nuclear Weapons Cybersecurity: NNSA Should Fully Implement Foundational
Cybersecurity Risk Management Practices" (GAO-22-104195)**

The Government Accountability Office recommends the Department of Energy's National Nuclear Security Administration (DOE/NNSA):

Recommendation 1: Promptly finalize Supplemental Directive 205.1, *Baseline Cybersecurity Program*, to include the most relevant federal cybersecurity requirements and review the directive at least every three years.

Management Response: Concur. Final update and issuance of the supplemental directive was delayed to complete and fully consider the results of a comprehensive, independent enterprise cybersecurity assessment commissioned by NNSA from the Institute for Defense Analysis (IDA). IDA completed their review and NNSA's Office of Information Management has prepared a revised draft Supplemental Directive 205.1, *Baseline Cybersecurity Program*, that includes the most relevant federal cybersecurity requirements. The draft must now undergo an Enterprise-wide internal review and approval process. The estimated date for issuing the final Supplemental Directive is April 30, 2023. Once issued, the Supplemental Directive will be scheduled for review every three years via RevCom.

Recommendation 2: Develop and maintain cybersecurity continuous monitoring strategies that address all elements from National Institute of Standards and Technology (NIST) guidance.

Management Response: Concur. Issuance of the updated Supplemental Directive 205.1, *Baseline Cybersecurity Program*, will address this recommendation. The updated Supplemental Directive includes requirements directing NNSA's Office of Information Management and the site contractors to develop and maintain cybersecurity continuous monitoring strategies that address all elements from NIST guidance. The estimated date for issuing the updated Supplemental Directive is April 30, 2023.

Recommendation 3: Identify and assign all risk management roles and responsibilities called for in NIST guidance.

Management Response: Concur. Issuance of the updated Supplemental Directive 205.1, *Baseline Cybersecurity Program*, will address this recommendation. The updated Supplemental Directive includes requirements directing NNSA's Office of Information Management and the site contractors to identify and assign all risk management roles and responsibilities called for in

**Appendix IX: Comments from the National
Nuclear Security Administration**

Enclosure

NIST guidance. The estimated date for issuing the updated Supplemental Directive is April 30, 2023.

Recommendation 4: Direct site contractors that have not done so maintain a site-wide cybersecurity risk management strategy that addresses all elements from NIST guidance and perform periodic reviews at least annually.

Management Response: Concur. Issuance of the updated Supplemental Directive 205.1, *Baseline Cybersecurity Program*, will address this recommendation. The updated Supplemental Directive includes requirements directing the site contractors to maintain a site-wide cybersecurity risk management strategy that addresses all elements from NIST guidance and perform periodic reviews at least annually. The estimated date for issuing the updated Supplemental Directive is April 30, 2023.

Recommendation 5: Identify the needed resources to implement foundational practices for the Operational Technology (OT) environment, such as by developing an OT activity business case for consideration in NNSA's planning, programming, budgeting, and evaluation process.

Management Response: Concur. Needed resources will be identified for developing an Operating Technology business case within Cybersecurity Improvement Plans and cyber program budget through the Planning, Programming, Budgeting and Evaluation process. The estimated date for completing this action is April 30, 2023.

Recommendation 6: Establish a cybersecurity risk management strategy for nuclear weapons information technology that includes all elements from NIST guidance.

Management Response: Concur. The Nuclear Enterprise Assurance Division, working with the various stakeholders within the Office of Defense Programs, will develop a cybersecurity risk management strategy for nuclear weapon information technology that includes appropriate elements from NIST guidance. The estimated date for completing this action is September 30, 2023.

Recommendation 7: Clarify and reinforce to the management and operating (M&O) contractors, such as by a policy flash or other communication, that they are required to monitor subcontractors' cybersecurity measures.

Management Response: Concur. NNSA's Office of Partnership and Acquisition Services will issue a Policy Flash after the updated Supplemental Directive 205.1, *Baseline Cybersecurity Program*, is released to notify the M&O contractors of the requirement to monitor subcontractors' cybersecurity measures. The estimated date for completing this action is May 31, 2023.

**Appendix IX: Comments from the National
Nuclear Security Administration**

Enclosure

Recommendation 8: Include performance criteria evaluating contractor oversight of subcontractor cybersecurity measures in the annual M&O contractor performance evaluation process.

Management Response: Concur. NNSA's Office of Partnership and Acquisition Services will include performance criteria evaluating contractor oversight of subcontractor cybersecurity measures in the annual M&O contractor performance evaluation process. The issuance of the updated Supplemental Directive 205.1, *Baseline Cybersecurity Program*, will address this recommendation. The estimated date for issuing the updated Supplemental Directive is April 30, 2023.

Recommendation 9: Ensure that Supplemental Directive 205.1, *Baseline Cybersecurity Program*, contains language requiring third-party validation of contractor and subcontractor cybersecurity measures.

Management Response: Concur. Issuance of the updated Supplemental Directive 205.1, *Baseline Cybersecurity Program*, will address this recommendation. The Supplemental Directive has been updated to clarify flow-down requirements to subcontractors to include directing third-party validation of contractor cybersecurity measures. The estimated date for issuing the updated Supplemental Directive is April 30, 2023.

Accessible Text for Appendix IX: Comments from the National Nuclear Security Administration

September 2, 2022

Ms. Allison B. Bawden
Director, Natural Resources
and Environment
U.S. Government Accountability Office
Washington, DC 20548

Dear Ms. Bawden:

Thank you for the opportunity to review the Government Accountability Office (GAO) draft report "Nuclear Weapons Cybersecurity: NNSA Should Fully Implement Foundational Cybersecurity Risk Management Practices" (GAO-22-104195). The Department of Energy's National Nuclear Security Administration (DOE/NNSA) recognizes the importance of cybersecurity, including nuclear weapon cybersecurity and for the associated equipment used for production and testing. As noted in the report, DOE/NNSA has taken positive steps to address the ever-growing digital threat to our programs.

DOE/NNSA appreciates GAO's observations on our efforts so far, and we welcome the auditors' recommendations for further enhancing our cybersecurity risk management practices. The attached Management Decision outlines the specific actions planned to address each recommendation. Our subject matter experts have also provided technical and general comments under separate cover for your consideration to enhance the clarity and accuracy of the report. If you have any questions about this response, please contact Dean Childs, Director, Audits and Internal Affairs, at (202) 836-3327.

Sincerely,

Jill Hruby

Enclosure

NATIONAL NUCLEAR SECURITY ADMINISTRATION

Management Decision

"Nuclear Weapons Cybersecurity: NNSA Should Fully Implement Foundational Cybersecurity Risk Management Practices" (GAO-22-104195)

The Government Accountability Office recommends the Department of Energy's National Nuclear Security Administration (DOE/NNSA):

Recommendation 1: Promptly finalize Supplemental Directive 205.1, Baseline Cybersecurity Program, to include the most relevant federal cybersecurity requirements and review the directive at least every three years.

Management Response: Concur. Final update and issuance of the supplemental directive was delayed to complete and fully consider the results of a comprehensive, independent enterprise cybersecurity assessment commissioned by NNSA from the Institute for Defense Analysis (IDA). IDA completed their review and NNSA's Office of Information Management has prepared a revised draft Supplemental Directive 205.1, Baseline Cybersecurity Program, that includes the most relevant federal cybersecurity requirements. The draft must now undergo an Enterprise-wide internal review and approval process. The estimated date for issuing the final Supplemental Directive is April 30, 2023. Once issued, the Supplemental Directive will be scheduled for review every three years via RevCom.

Recommendation 2: Develop and maintain cybersecurity continuous monitoring strategies that address all elements from National Institute of Standards and Technology (NIST) guidance.

Management Response: Concur. Issuance of the updated Supplemental Directive 205.1, Baseline Cybersecurity Program, will address this recommendation. The updated Supplemental Directive includes requirements directing NNSA's Office of Information Management and the site contractors to develop and maintain cybersecurity continuous monitoring strategies that address all elements from NIST guidance. The estimated date for issuing the updated Supplemental Directive is April 30, 2023.

Recommendation 3: Identify and assign all risk management roles and responsibilities called for in NIST guidance.

Management Response: Concur. Issuance of the updated Supplemental Directive 205.1, Baseline Cybersecurity Program, will address this recommendation. The updated Supplemental Directive includes requirements directing NNSA's Office of Information Management and the site contractors to identify and assign all risk

management roles and responsibilities called for in NIST guidance. The estimated date for issuing the updated Supplemental Directive is April 30, 2023.

Recommendation 4: Direct site contractors that have not done so maintain a site-wide cybersecurity risk management strategy that addresses all elements from NIST guidance and perform periodic reviews at least annually.

Management Response: Concur. Issuance of the updated Supplemental Directive 205.1, Baseline Cybersecurity Program, will address this recommendation. The updated Supplemental Directive includes requirements directing the site contractors to maintain a site-wide cybersecurity risk management strategy that addresses all elements from NIST guidance and perform periodic reviews at least annually. The estimated date for issuing the updated Supplemental Directive is April 30, 2023.

Recommendation 5: Identify the needed resources to implement foundational practices for the Operational Technology (OT) environment, such as by developing an OT activity business case for consideration in NNSA's planning, programming, budgeting, and evaluation process.

Management Response: Concur. Needed resources will be identified for developing an Operating Technology business case within Cybersecurity Improvement Plans and cyber program budget through the Planning, Programming, Budgeting and Evaluation process. The estimated date for completing this action is April 30, 2023.

Recommendation 6: Establish a cybersecurity risk management strategy for nuclear weapons information technology that includes all elements from NIST guidance.

Management Response: Concur. The Nuclear Enterprise Assurance Division, working with the various stakeholders within the Office of Defense Programs, will develop a cybersecurity risk management strategy for nuclear weapon information technology that includes appropriate elements from NIST guidance. The estimated date for completing this action is September 30, 2023.

Recommendation 7: Clarify and reinforce to the management and operating (M&O) contractors, such as by a policy flash or other communication, that they are required to monitor subcontractors' cybersecurity measures.

Management Response: Concur. NNSA's Office of Partnership and Acquisition Services will issue a Policy Flash after the updated Supplemental Directive 205.1, Baseline Cybersecurity Program, is released to notify the M&O contractors of the requirement to monitor subcontractors' cybersecurity measures. The estimated date for completing this action is May 31, 2023.

Recommendation 8: Include performance criteria evaluating contractor oversight of subcontractor cybersecurity measures in the annual M&O contractor performance evaluation process.

Management Response: Concur. NNSA's Office of Partnership and Acquisition Services will include performance criteria evaluating contractor oversight of subcontractor cybersecurity measures in the annual M&O contractor performance evaluation process. The issuance of the updated Supplemental Directive 205.1, Baseline Cybersecurity Program, will address this recommendation. The estimated date for issuing the updated Supplemental Directive is April 30, 2023.

Recommendation 9: Ensure that Supplemental Directive 205.1, Baseline Cybersecurity Program, contains language requiring third-party validation of contractor and subcontractor cybersecurity measures.

Management Response: Concur. Issuance of the updated Supplemental Directive 205.1, Baseline Cybersecurity Program, will address this recommendation. The Supplemental Directive has been updated to clarify flow-down requirements to subcontractors to include directing third-party validation of contractor cybersecurity measures. The estimated date for issuing the updated Supplemental Directive is April 30, 2023.

Appendix X: GAO Contacts and Staff Acknowledgments

GAO Contacts

Allison B. Bawden, (202) 512-3841, bawdena@gao.gov

David B. Hinchman, (214) 777-5719, hinchmand@gao.gov

Staff Acknowledgments

In addition to the contact named above, William Hoehn (Assistant Director), Josh Leiling (Assistant Director), Julia T. Coulter (Analyst-in-Charge), Corey Evans, Camille Pease, Maria Stattel, Vijay A. D'Souza, Antoinette Capaccio, Steven Putansu, Caitlin Scoville, Ellen Fried, and Dan Royer made key contributions to this report.

Also contributing to this report were Nathan Anderson, Ben Atwater, Tommy Baril, Penney Harwell Caramia, Raj Chitikila, Leslie Gordon, Madhav Panwar, and Tina Won Sherman.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548



Please Print on Recycled Paper.