U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

June 12, 2023

Congressional Addressees

Nuclear Weapons Cybersecurity: Status of NNSA's Inventory and Risk Assessment Efforts for Certain Systems

Within the U.S. government, the Department of Energy's (DOE) National Nuclear Security Administration (NNSA) is charged with maintaining, modernizing, and securing the nation's nuclear weapons stockpile. Digital systems are increasingly being integrated into nuclear weapons and into activities and operations across the NNSA's nuclear security enterprise.[1] There is potential for these digital systems to be hacked, corrupted, or subverted by malicious actors, and NNSA has stated that securing its digital assets is an agency priority.

In the context of the nuclear security enterprise, NNSA generally characterizes IT contained within a warhead or bomb, including model versions of a warhead or bomb, as nuclear weapons IT.[2] An example of a nuclear weapons IT system is the weapon control unit inside the B61-12 gravity bomb.[3] NNSA uses operational technologies (OT) in the processes, equipment, materials, and products employed in the production of nuclear weapons.[4] Examples of OT systems include building safety systems (e.g., fire suppression systems) or an additive manufacturing system used to print polymer components.

[1]NNSA's nuclear security enterprise comprises a network of eight government-owned, contractor-operated national security laboratories and nuclear weapons production facilities that provide the research, development, testing, and production capabilities needed to maintain and modernize our nation's nuclear weapons stockpile and related infrastructure.

[2]According to NNSA officials, nuclear weapons IT is defined as the information system or components of an information system integral to a nuclear weapon; surrogates for nuclear weapons used in development, test, or training; and equipment connecting to nuclear weapons or their surrogates, including war reserve units, developmental units, weapon components, test units, trainer units, and weapon operational support equipment (e.g., systems that are directly involved in operational testing, configuration, security, and safety throughout the life cycle).

[3]All nuclear weapons in the U.S. stockpile are designated as either a warhead or a bomb. Warheads are weapons that have certain engineering requirements because they must interface with a launch or delivery system. Bombs are weapons that do not have these interface requirements, such as gravity bombs and atomic demolition munitions (now retired and dismantled). The weapon control unit is the primary controller that provides information and detonation management functionality for gravity bombs.

[4]According to the Department of Energy, OT is any hardware or software that detects or causes a change through the direct monitoring or control of physical devices, processes, or events. See Department of Energy, *Department of Energy Cybersecurity Program,* Order 205.1C (Washington, D.C.: Feb. 3, 2022).

Federal law and policies require that NNSA establish a program to manage cybersecurity risk.[5] NNSA's Office of the Chief Information Officer and Information Management (NA-IM) is broadly responsible for implementing cybersecurity within NNSA and is directly responsible for implementing and managing cybersecurity risks to OT systems. NNSA's Nuclear Enterprise Assurance (NEA) Division, located within the Office of Defense Programs (Defense Programs)—which oversees stockpile sustainment and weapons development—has primary responsibility for managing cybersecurity risks to nuclear weapons IT systems and shares responsibility with NA-IM for OT risk management. NA-IM and Defense Programs share responsibility for managing risks to building systems and industrial control processes, and Defense Programs also manages risks to equipment and processes used to produce weapons and weapons components.

NNSA carries out its mission through a nuclear security enterprise composed of a nationwide network of government-owned, contractor-operated national security laboratories and nuclear weapons production facilities. Specifically, NNSA oversees

- three national security laboratories that design and, in some cases, fabricate nuclear and nonnuclear components—Lawrence Livermore in California, Los Alamos in New Mexico, and Sandia in New Mexico and California;
- three production sites that fabricate additional nuclear and nonnuclear components—Y-12 National Security Complex in Tennessee, Kansas City National Security Campus in Missouri, and the Savannah River Site in South Carolina;
- an additional production site, the Pantex Plant in Texas, that assembles, disassembles, and repairs nuclear weapons; and
- a site that conducts experiments in support of the national security laboratories—the Nevada National Security Site in Nevada.

According to NNSA officials, OT systems are present at each site, and nuclear weapon IT systems are present at most of the sites. NNSA's cybersecurity requirements are applicable to the contractors that manage and operate these sites through agency directives that are incorporated into their contracts and, thus, these requirements apply to the nuclear weapons IT and OT systems at these sites.

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 asked to perform related work. In September 2022, we issued a report that assessed NNSA's nuclear weapons cybersecurity efforts from a broad organizational and planning perspective in these two environments.[6] We made nine recommendations to NNSA to improve cybersecurity risk management, all of which NNSA agreed with. As of May 2023, NNSA had identified actions to address our recommendations but had not fully implemented any of them. This report describes

[5]Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073; Office of Management and Budget, *Managing Information as a Strategic Resource,* OMB Circular A-130 (Washington, D.C.: July 27, 2016); DOE Order 205.1C; and National Nuclear Security Administration, *Baseline Cybersecurity Program*, Supplemental Directive (SD) 205.1 (Washington, D.C.: July 6, 2017).

[6]GAO, *Nuclear Weapons Cybersecurity: NNSA Should Fully Implement Foundational Cybersecurity Risk Management Practices,* GAO-22-104195 (Washington, D.C.: Sept. 22, 2022).

the steps that NNSA has taken to inventory the range of systems in the OT and nuclear weapons IT environments and to assess and mitigate the cyber risks to such systems.

To describe the steps that NNSA has taken to inventory the range of systems at risk in the OT and nuclear weapons IT environments, assess cybersecurity risks to these systems, and identify cybersecurity risk mitigations, we reviewed DOE and NNSA directives that direct NNSA and its site contractors to establish cybersecurity risk management frameworks that address these environments. We reviewed NNSA and site documents, such as system inventory lists or OT assessment reports, to describe the range of OT and nuclear weapons IT systems that NNSA and its contractors have inventoried. We also reviewed documentation, such as program protection plans for certain weapons, site cybersecurity improvement plans, and NNSA guidance to describe risks to OT and nuclear weapons IT systems that NNSA has identified and any corrective action plans to mitigate those risks.

We also interviewed knowledgeable officials from NA-IM and Defense Programs to understand their perspectives on the extent to which NNSA has identified the full scope of its OT and nuclear weapons IT systems, assessed risks to these systems, and identified risk mitigations. We also interviewed federal officials and contractor representatives at DOE's Idaho National Laboratory to learn more about the process of OT assessments. We reviewed responses to written questions sent to contractor representatives at each of the sites to obtain the most current information about the status of OT assessments.

We conducted this performance audit from October 2022 to June 2023 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.

NNSA Is in the Early Stage of Efforts to Inventory OT and Nuclear Weapons IT Systems and to Assess and Mitigate Risks

OT Environment

NNSA's efforts to address cybersecurity at the system level in the OT environment remain in the early stages of development and implementation. In our September 2022 report, we noted that NNSA has made limited progress—after several years of effort—to implement risk management practices that would help it inventory OT systems and assess and mitigate the risks to such systems.[7] NNSA has estimated that there could be hundreds of thousands of OT systems at sites across the nuclear security enterprise.

[7]GAO-22-104195.

NNSA is taking some steps as a precursor to creating an inventory of systems in its OT environment and assessing and mitigating the risks to such systems.[8] These steps include:

- **Developing the Operational Technology Assurance (OTA) Guidebook.** NNSA is developing a guidebook for NNSA and its sites to identify and prioritize actions for reducing risk and to align various approaches to managing that risk. The December 2022 version of the guidebook presents a systemic process for identifying, assessing, and managing OT digital risk.[9] According to the guidebook and NNSA officials, it is a living document that is updated periodically to incorporate lessons learned.

- **Creating OT courses and training staff.** NNSA officials told us that they had created a series of three OT training courses that range from introductory to advanced level. They have conducted training sessions for personnel and contractors at each of the sites to guide and set the expectations for applying the guidebook to day-to-day, site-level business operations. These courses include approaches to inventorying OT systems and addressing potential risks to such systems, according to NNSA officials.

NNSA's efforts to inventory OT systems, and assess and mitigate risks to them, are still in their early stages and, as of May 2023, have been limited in scope. The two main actions that NNSA is taking include:

- **Identifying OT systems associated with the most critical capability at each site.** NNSA officials told us that they surveyed senior management within NNSA and at each of NNSA's sites to identify the OT capability at each site that was most critical to NNSA's mission. For example, at Y-12, NNSA identified systems used for manufacturing and certification of weapons-related material or components as the site's most critical capability. The reasoning behind this was that its loss would affect its ability to manufacture and certify components. NNSA officials told us in November 2022 that the sites planned to conduct a system-of-systems breakdown of their priority capability to create an inventory of OT systems associated with that capability. Officials stated that, following the system-of-systems breakdown of the priority site capability, the site would assess and identify mitigations for the risks to those systems.

- **Conducting assessments of OT systems.** Most NNSA sites have selected a single OT system or system component to assess for risk and as a learning exercise, according to site reports. According to NNSA officials, each of the sites selected the OT system to evaluate based on its relationship to the most critical capability and additional analysis. According to a representative of one site, they chose to focus on a single system or component to meet three important goals—learn the OTA review process, conduct a deep dive assessment of key technologies, and adapt the OTA process to best fit their needs.

[8]In our September 2022 report, we noted that NNSA officials said that there may be hundreds of thousands of systems at NNSA sites in the OT environment. One site—Kansas City—was estimated to have approximately 46,000 systems at that time that were involved in the design and manufacture of weapons components—not including systems used to control building functions, according to these officials. As of May 2023, NNSA officials did not have an updated estimate of OT systems at the Kansas City site but said that the estimate of 46,000 systems would likely change as OT efforts progress.

[9]NNSA's approach is based on a long-standing OT risk management framework developed by Idaho National Laboratory and that is being used in the government and private sectors to manage the risk to OT systems.

According to our review of site reports, these assessments have generally begun with a 3-day kickoff event at the site. NNSA officials and site representatives use the kickoff to begin an information collection process to identify personnel roles and subject matter expertise, in addition to resource material and technical tools required to conduct a successful assessment. Afterward, the sites continue to assess the system until completion of the final report, according to site reports, which can take up to a year.

As of May 2023, one site—Nevada—has completed a system-of-systems breakdown of its most critical OT capability, assessed risks to each system in that capability, and identified risk mitigations to those systems.

Assessments of select OT systems or components have been completed at Los Alamos and Y-12, as of May 2023. The assessed systems or components were chosen based on their relevance to the site's most critical capability, according to these assessments or related documentation. In general, the completed assessment reports and related documentation that we reviewed identified some risks to the represented systems or components, but only Nevada's assessment addressed mitigation actions.

Assessments of select OT systems have been initiated at four other NNSA sites—Kansas City, Livermore, Pantex, and Savannah River—but have not been completed as of May 2023. A representative for Sandia stated that an assessment had been initially scheduled for May 2023 but had been delayed—likely to September 2023.

Nuclear Weapons IT Environment

NNSA's efforts to address cybersecurity at the system level in the nuclear weapons IT environment are also in their early stages. NNSA officials do not currently have an estimate of the number of systems that may be in the nuclear weapons IT environment. However, NNSA officials told us that the scope of nuclear weapons IT systems potentially at risk is smaller compared with the OT environment. NNSA officials also told us that risks vary from one nuclear weapon type to another, in part because some nuclear weapons currently in service were developed and introduced into the stockpile decades ago—and include little IT.[10] On the other hand, newer and more modern weapons are slated to begin entering the stockpile after 2030, and their designs may include more IT than legacy weapons' designs.[11] In addition, IT systems may exist in configurations that support nuclear weapon activities, such as stockpile surveillance; flight testing units; testing units for compatibility with Department of Defense (DOD) systems; and training, among other activities.

NNSA has begun a number of efforts to facilitate the creation of an inventory of nuclear weapons IT systems and to assess and mitigate the cyber risks to such systems, including:

- **Defining nuclear weapons IT**. NNSA officials told us in November 2022 that NNSA had not yet created a nuclear weapons IT inventory because the agency had not issued guidance to formally define the term. As of May 2023, NNSA does not have an official definition for nuclear weapons IT. NNSA officials told us that they expect to define the term in both the agency's planned revision of its cybersecurity directive, SD 205.1,

[10]Older weapons designs currently in the stockpile are the B61, W76, W78, W80, B83, W87, and W88 and are considered legacy weapons. Over time, some of these weapons have been modified into different versions, such as the W76-1 and W76-2, which are modifications of the original W76-0.

[11]NNSA has two modernization programs under way—the W87-1 and W93—that include newer design features.

Baseline Cybersecurity Program, and in its new IT management directive, SD 200.1, *Information Resources Management*.[12] In April 2023, NNSA officials stated that the planned issuance date for SD 205.1 had been postponed from April 2023 to October 2023. In May 2023, NNSA officials said that they could not provide an estimate for when either SD 200.1 or SD 205.1 would be issued. NNSA officials said that once the agency formally defines nuclear weapons IT, they will review weapon systems to identify those that may formally be considered nuclear weapons IT.[13]

- **Developing a cybersecurity risk management framework**. As we reported in September 2022, NNSA is developing, but does not yet have, a cybersecurity risk management framework for the nuclear weapons IT environment.[14] NNSA anticipates that it will finalize its cybersecurity risk management requirements, which are intended to align requirements with National Institute of Standards and Technology (NIST) recommended system security engineering principles, by the end of fiscal year 2024.[15] NNSA officials said that they expect that establishing a cybersecurity risk management framework will help facilitate the assessment and mitigation of cyber risks to nuclear weapons IT.

- **Performing a gap analysis**. To align NNSA's cybersecurity risk management framework with existing engineering processes, in November 2021, NNSA conducted a gap analysis for nuclear weapons modernization programs that identified a significant amount of ambiguity in cybersecurity risk management roles and responsibilities within NNSA and at the sites. As a result, over the course of calendar year 2022, NNSA gathered experts from within NNSA, the laboratory and production sites, and DOD, to conduct four collaborative exercises to clarify roles and responsibilities. Participants took a fictional weapon through its life cycle to help clarify risk domains and boundaries, risk ownership, risk management coordination across boundaries, and overall risk integration to support risk decisions.

  NNSA will use the results from these exercises to implement the nuclear weapons IT cybersecurity risk management framework currently being drafted and to develop related guidance, according to an NNSA exercise summary. For example, NNSA found that it does not have realistic cybersecurity threat models for its weapons—an important element of cybersecurity risk management, according to NIST guidance.[16] In response, NNSA officials said that they were developing a threat model that could be applied to both older and newer weapons. According to these officials, the model will be ready to be assessed by an independent expert third party in June 2023.

[12]In our September 2022 report, we noted that this directive had not been updated since 2017.

[13]Though NNSA has not created a nuclear weapons IT inventory, NNSA has detailed information on each component and system within a nuclear weapon.

[14]GAO-22-104195.

[15]National Institute of Standards and Technology, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, Special Publication (SP) 800-160, Volume 2 (Gaithersburg, M.D.: November 2019).

[16]NIST defines threat modeling as a form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment.

- **Revising internal weapons program guidance.** NNSA is also using the results of the exercises to further align cybersecurity roles, responsibilities, and decision-making in the risk management framework with the weapons life cycle, according to NNSA documents. NNSA officials stated that they had revised some internal guidance and procedures to incorporate cybersecurity risk management requirements, and they noted that completion and issuance of the guidance and procedures would be delayed. Specifically, these officials told us that in March 2023, the NNSA Deputy Administrator had instituted a pause on revisions to all NNSA guidance as NNSA undertakes an agency-wide reevaluation of the guidance and procedures that it uses to manage its contractors.[17] NNSA officials said that, as the pause is gradually lifted, they would issue revised guidance and procedures that incorporate cybersecurity risk assessment and mitigation provisions. NNSA officials said that they intended to issue this guidance by the end of fiscal year 2024.

In the absence of formal guidance and procedures, NNSA is taking some preliminary steps to identify and assess risks to nuclear weapons IT systems associated with specific nuclear weapon types.

Regarding nuclear weapon systems with older designs, such as the W78 or the W76-0, NNSA officials said that they have conducted preliminary reviews to assess them for nuclear weapons IT. From these reviews, NNSA officials said that they had determined that, in general, due to the weapons' age and reliance upon older technology, they contain little nuclear weapons IT that is at risk. While NNSA officials said that efforts to document the results of such assessments were still early and ongoing, they would eventually like to develop a technical risk register (i.e., a management tool that tracks and manages cybersecurity risks) across older systems. However, NNSA officials could not estimate when such an effort would be initiated or completed.

Regarding nuclear weapon systems in development, such as the W80-4, W87-1, and W93, NNSA officials said that each program is considering approaches to managing cybersecurity risks as part of the weapon design and development process. Specifically, NNSA officials and Sandia representatives said that the W80-4 program had received approval to implement a tailored version of the risk management framework in its development. According to NNSA officials and Sandia representatives, the W87-1 federal program manager was evaluating the efficacy of the requirements in the cybersecurity risk management framework to the development of that system. Lastly, officials managing the W93 program told us that the program was still in an early design stage and that engineers focused on cybersecurity and digital assurance would be part of engineering teams planned for the summer of 2023.

Agency Comments

We provided a draft of this product to NNSA for review and comment. NNSA provided technical comments, which we incorporated, as appropriate.

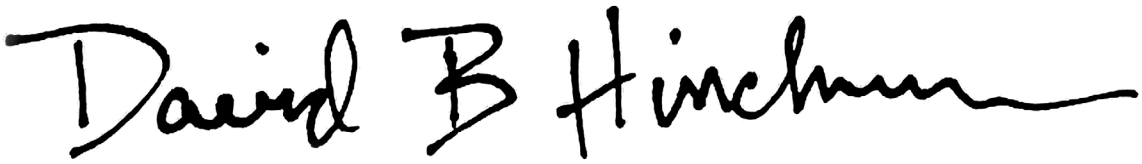
- - - - -

[17]NNSA's Enhanced Mission Delivery Initiative is intended to improve NNSA and contractor contract structure; personnel policies; and work environment, among other things, according to the NNSA Administrator.

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

If you or your staff have any questions about this report, please contact us at (202) 512-3471 or BawdenA@gao.gov; or (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 key contributions to this report include William Hoehn (Assistant Director), Josh Leiling (Assistant Director), Julia T. Coulter (Analyst in Charge), Corey Evans, Antoinette Capaccio, Andrew Stavisky, and Caitlin Scoville. Also contributing to this report were Carol Cimitile, Joe Kirschbaum, John Ortiz, Bill Reinsberg, W. William Russell, and James Walker.

Allison B. Bawden
Director, Natural Resources and Environment



David B. Hinchman
Director, Information Technology and Cybersecurity

List of Addressees

The Honorable Jack Reed
Chairman
The Honorable Roger Wicker
Ranking Member
Committee on Armed Services
United States Senate

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

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

The Honorable Chuck Fleischmann
Chair
The Honorable Marcy Kaptur
Ranking Member
Subcommittee on Energy and Water Development and Related Agencies
Committee on Appropriations
House of Representatives

The Honorable Michael Turner
House of Representatives

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