UKRAINE
DOE Could Better Assess Fraud Risks and Formalize Its Transition Plans for Nuclear Security and Safety Efforts

Report to Congressional Committees

June 2025

GAO-25-108444

United States Government Accountability Office

Accessible Version

GAO Highlights

For more information, contact Allison Bawden at bawdena@gao.gov or Nagla'a El-Hodiri at elhodirin@gao.gov.
Highlights of GAO-25-108444, a report to congressional committees

Ukraine

DOE Could Better Assess Fraud Risks and Formalize Its Transition Plans for Nuclear Security and Safety Efforts

Why GAO Did This Study

Russia's 2022 invasion of Ukraine has jeopardized nuclear security and safety there. Congress appropriated more than $113 billion in supplemental funding, including $161.3 million for NNSA to respond to the situation. The conditions on the ground in Ukraine have increased fraud risk, and the history of U.S. nuclear security assistance to Ukraine has raised questions about NNSA's plans to transition responsibility to Ukrainian organizations to sustain these efforts.

The Consolidated Appropriations Act, 2023, includes a provision for GAO to conduct oversight of the supplemental funding. This report addresses (1) agency efforts to support nuclear and radiological security and safety in Ukraine, (2) NNSA's steps to mitigate fraud risks, and (3) NNSA's planning to transition responsibility for relevant efforts to Ukrainian partners.

GAO reviewed agency documents, including procedures for mitigating fraud risk, and a sample of its contracts for Ukraine-related efforts. GAO also interviewed U.S. agency officials and received written responses from Ukrainian agencies. This is a public version of a Controlled Unclassified Information (CUI) report issued in April 2025. Information that NNSA deemed CUI has been omitted.

What GAO Recommends

GAO recommends that DOE (1) require timely fraud risk assessments for programs that experience structural changes or a changed operating environment or add new services, and (2) formalize plans for transitioning responsibility to Ukrainian partners, as appropriate. DOE agreed with the recommendations.

What GAO Found

The Department of Energy's (DOE) National Nuclear Security Administration (NNSA) leads U.S. efforts to support nuclear and radiological security and safety in Ukraine. NNSA has used its supplemental funding for efforts such as providing security upgrades at nuclear facilities, training for nuclear incident response, and countering nuclear smuggling. The Departments of Defense and State and the Nuclear Regulatory Commission used supplemental or regular appropriations, or a combination, to conduct a smaller range of related activities. These included providing radiation detection equipment and helping reduce Ukrainian nuclear reactors' dependency on Russian nuclear fuels.

Truck Moving Nuclear Safety Equipment in Ukraine

Source: National Nuclear Security Administration (NNSA). | GAO-25-108444

While NNSA took steps to manage fraud risk at the individual contract level, it did not conduct a program-level fraud risk assessment tailored to its nuclear and radiological security and safety efforts in Ukraine. A tailored fraud risk assessment is a leading practice for effective antifraud strategy, according to GAO's Fraud Risk Framework. DOE guidance generally directs offices to follow the framework's leading practices. However, it does not include specific guidance directing offices to conduct assessments outside of DOE's annual agency-wide fraud risk assessment cycle when there are structural changes to the program, changes to the operating environment, or new services added—as happened for programs responding to the invasion of Ukraine. By updating its guidance with such direction, DOE will better ensure its offices consistently assess emerging fraud risks and design appropriate mitigation measures before obligating taxpayer funds.

NNSA intends to transition responsibility for certain nuclear security efforts to Ukrainian partners but has not documented transition plans for these efforts. Doing so is a program management leading practice. NNSA officials said uncertainties in operating conditions as a result of the ongoing conflict complicate transition planning. However, formalizing transition plans, which NNSA can adapt as operating conditions change, would provide NNSA, Congress, and taxpayers stronger assurance that Ukrainian partners can sustain the efforts that the U.S. invested in after U.S. support ends.

Contents

Tables

Figures

Abbreviations

ANL	Argonne National Laboratory
CHIPS	Creating Helpful Incentives to Produce Semiconductors
CTCP	Office of Counterterrorism and Counterproliferation
DOE	Department of Energy
DNN	Office of Defense Nuclear Nonproliferation
DOD	Department of Defense
ERM	Enterprise Risk Management
FAR	Federal Acquisition Regulation
GMS	Office of Global Material Security
IAEA	International Atomic Energy Agency
IDIQ	indefinite delivery, indefinite quantity
ISN	Bureau of International Security and Nonproliferation
LLC	limited liability company
M&O	management and operating
NNSA	National Nuclear Security Administration
NRC	Nuclear Regulatory Commission
NSDD	Nuclear Smuggling Detection and Deterrence
OMB	Office of Management and Budget
ORS	Office of Radiological Security
PNNL	Pacific Northwest National Laboratory
RANET	Response and Assistance Network
STARS	Standard Accounting and Reporting System
WMD	weapons of mass destruction

June 12, 2025

Congressional Committees

Russia's February 2022 invasion of Ukraine has caused tremendous loss of life, created a humanitarian crisis, threatened democracy, exacerbated global challenges such as food insecurity, and jeopardized nuclear security and safety. In particular, the invasion has challenged Ukraine's ability to sustain effective security at sites with nuclear and radioactive material, maintain effective capabilities to counter smuggling of nuclear and radioactive materials, and safely operate its nuclear power plants. In response to the invasion, Congress appropriated more than $113 billion under four Ukraine supplemental appropriations acts from March through December 2022.[1] These appropriations included $161.3 million for the National Nuclear Security Administration's (NNSA) Office of Defense Nuclear Nonproliferation (DNN), within the Department of Energy (DOE), to "respond to the situation in Ukraine and for related expenses."[2]

In the decades before Russia's invasion, NNSA and other key U.S. agencies, including the Departments of Defense (DOD) and State and the Nuclear Regulatory Commission (NRC), worked with Ukrainian partner organizations to improve nuclear and radiological security and safety there.[3] Since the invasion, these agencies have continued to support such efforts, funded by regular and supplemental appropriations. Of the key agencies that received supplemental appropriations for these efforts, NNSA received the largest amount.

The speed with which funding has been disbursed, combined with the active conflict zone in Ukraine, have contributed to an elevated fraud risk associated with U.S.-funded efforts there. Combined with NNSA's reliance

[1]For the purposes of our reporting objectives, we use the phrase "Ukraine supplemental appropriations acts" and "supplemental appropriations" to refer to applicable divisions of the following public laws: Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, div. N, 136 Stat. 776 (enacted March 15, 2022); Additional Ukraine Supplemental Appropriations Act, 2022, Pub. L. No. 117-128, 136 Stat. 1211 (enacted May 21, 2022); Continuing Appropriations and Ukraine Supplemental Appropriations Act, 2023, Pub. L. No. 117-180, 136 Stat. 2114 (2022) (enacted September 30, 2022); and Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, div. M, 136 Stat. 5189 (2022) (enacted December 29, 2022).

[2]NNSA is a separately organized agency within DOE. Congress appropriated NNSA $35 million in September 2022 and $126.3 million in December 2022. These amounts are part of a total of $491 million that Congress appropriated to DOE through the Ukraine supplemental appropriations acts for energy programs and nuclear security. According to DOE, the funds appropriated for energy programs will go to support research on advanced nuclear reactors and fuels. We reported on DOE's expenditure of these funds in *Ukraine: Status and Use of Supplemental U.S. Funding, as of First Quarter, Fiscal Year 2024*, GAO-24-107232 (Washington, D.C.: May 30, 2024).

[3]We define "key agencies" as NNSA, State, NRC, and DOD. We selected these four agencies based on our review of agency and interagency documents, interviews with agency officials, and prior GAO reports. In addition to these key agencies, we reviewed the efforts of the International Atomic Energy Agency, an autonomous international organization to which some of the Ukraine supplemental funding appropriated to NNSA was obligated (this agency is funded by member states, including the U.S.). We excluded U.S. agencies with smaller roles, such as the Department of Health and Human Services, Department of Homeland Security, and Environmental Protection Agency.

on contractors and its history of lax contractor oversight,[4] and Ukraine's history of corruption, these factors raise concerns about fraud risk management. In addition, the history of U.S. nuclear security assistance to Ukraine over the past several decades has raised questions about NNSA's plans to transition responsibility to Ukrainian partner organizations to effectively sustain these efforts at some point in the future without continued U.S. assistance.

Division M of the Consolidated Appropriations Act, 2023, includes a provision for us to conduct oversight of the assistance provided in the Ukraine supplemental appropriations acts. Our report is part of a series of reports evaluating U.S. agencies' implementation of these funds in response to the crisis in Ukraine. In this report, we (1) describe efforts NNSA and other key agencies have undertaken or planned to support nuclear and radiological security and safety in Ukraine, (2) examine the extent to which NNSA has taken steps to mitigate fraud risks in its efforts for Ukraine that were funded through supplemental appropriations, and (3) examine the extent to which NNSA has planned to transition relevant efforts to Ukrainian partners and ensure their sustainability.

This report is a public version of a Controlled Unclassified Information (CUI) report that we issued in April 2025.[5] The National Nuclear Security Administration deemed some of the information in our April 2025 report to include CUI, which must be protected from public disclosure. Therefore, this report omits some information about certain program activities. Although the information provided in this report is more limited, the report addresses the same objectives as the CUI report and uses the same methodology.

To describe efforts NNSA and other key agencies have undertaken to support nuclear and radiological security and safety in Ukraine, we reviewed agency budget and planning documents and annual reports and interviewed officials from these agencies. We took steps to assess the reliability of the funding data and found them to be sufficiently reliable for the purposes of describing the support provided. We identified nuclear and radiological security and safety risks driving these agencies' efforts by (1) reviewing intelligence assessments produced by DOE and written responses from Ukrainian agencies that we were able to obtain by working through State and (2) interviewing NNSA and DOE officials. We interviewed Ukrainian officials to understand how they prioritize the requests they make for support from these agencies.

To examine the extent to which NNSA has taken steps to mitigate fraud risks in its efforts funded through the supplemental appropriations, we reviewed agency documents and interviewed agency officials and

[4]We designated aspects of DOE's contract management as a high-risk area for the government in 1990 because DOE's record of inadequate management and oversight of contractors left the department vulnerable to fraud, waste, abuse, and mismanagement. GAO, *Government Financial Vulnerability: 14 Areas Needing Special Review*, GAO/OCG-90-1 (Washington, D.C.: Jan. 23, 1990). We subsequently narrowed the focus of this high-risk designation to DOE's Office of Environmental Management and the National Nuclear Security Administration. GAO, *High-Risk Series: An Update,* GAO-09-271 (Washington, D.C.: Jan. 22, 2009). Additionally, in its fiscal year 2018 identification of management challenges, DOE's Office of Inspector General (OIG) added subcontract management as a component of its previously identified management challenges for DOE contract oversight, in part because the OIG's investigative work and referrals to the OIG hotline identified continued vulnerabilities from inadequate oversight of subcontracts. Department of Energy, Office of Inspector General, *Management Challenges at the Department of Energy – Fiscal Year 2018*, DOE-OIG-18-09 (Washington, D.C.: Nov. 27, 2017). Each year, the DOE OIG identifies management challenges at the department.

[5]GAO, *Ukraine: DOE Could Better Assess Fraud Risks and Formalize Its Transition Plans for Nuclear Security and Safety Efforts*, GAO-25-107015SU (Washington, D.C.: Apr. 16, 2025). We also issued a separate classified annex to the CUI report that provides additional details on the nuclear and radiological security and safety risk environment in Ukraine and about certain actions NNSA is taking in response: GAO, *Classified Annex for GAO-25-107015SU: Additional Details on Nuclear and Radiological Security and Safety Risks in Ukraine*, GAO-25-107768C (Washington, D.C.: Apr. 16, 2025).

contractors. Specifically, we reviewed DOE and NNSA guidance and procedures for mitigating fraud risk.[6] We also reviewed DOE and NNSA documents and interviewed agency officials about NNSA's overall fraud mitigation approach for its Ukraine-related contracts. We collected information on the contract oversight and fraud risk mitigation approaches that NNSA officials and contractor representatives used on individual contracts by reviewing a nongeneralizable sample of eight of NNSA's largest contracts that involved subcontracted work; examining documentation associated with each, such as cost-tracking spreadsheets, technical review documents, and photographs of delivered equipment and identifying characteristics, such as serial numbers; and interviewing NNSA officials and contractors. We compared NNSA's efforts against leading practices in GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework),[7] which contains leading practices that managers are directed to implement by the Office of Management and Budget (OMB).[8]

To examine the extent to which NNSA has planned to transition relevant efforts to Ukrainian partners and ensure their sustainability, we focused on NNSA programs that used supplemental appropriations funding for longer term efforts, such as those that provide equipment, training, and other services to Ukrainian partner organizations.[9] We reviewed relevant NNSA program transition and sustainment plans and interviewed NNSA program officials. We compared NNSA's plans against leading practices for program management.

The performance audit upon which this report is based was conducted from September 2023 to April 2025 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. We subsequently worked with DOE from April 2025 through May 2025 to prepare this public version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

Background

Nuclear and Radiological Security and Safety

Terminology related to nuclear and radiological security and safety includes the following:[10]

[6]We focused this objective on NNSA because, of the key agencies we examined, it received the most supplemental funding for nuclear and radiological security and safety in response to the invasion of Ukraine.

[7]GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 2015).

[8]Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control*, OMB Circular No. A-123 (July 15, 2016).

[9]We selected NNSA for our focus because it is the lead U.S. agency for nuclear and radiological security and safety efforts in Ukraine. We did not focus on efforts intended to be temporary, such as providing short-term emergency response support.

[10]The following definitions are based primarily on the International Atomic Energy Agency's (IAEA) Nuclear Safety and Security Glossary, with input from the agencies that commented on the report. See *IAEA Nuclear Safety and Security Glossary: Terminology Used in Nuclear Safety, Nuclear Security, Radiation Protection and Emergency Preparedness and Response, Interim* edition (Vienna, Austria: 2022).

- **Nuclear security** is the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer, or other malicious acts involving nuclear material, other radioactive substances, or their associated facilities. Nuclear security includes physical protection of such material. It generally focuses on preventing intentional actions by people that could cause or threaten harm.
- **Radiological security** refers specifically to security of nonfissile radioactive material such as cesium-137, cobalt-60, and strontium-90. Such material may be used for medical, industrial, and research purposes, such as treating cancer and sterilizing food and medical instruments. In the wrong hands, it could be used in a radiological dispersal device, also referred to as a "dirty bomb." Depending on the type, form, amount, and concentration of radioactive material used, such a device could expose nearby individuals to ionizing radiation and increase their long-term risks of cancer.[11] It could also lead to socioeconomic consequences such as relocations, billions of dollars in cleanup costs, and fatalities resulting from evacuations.[12]
- **Nuclear safety** encompasses the broader issue of harmful consequences to people (and the environment) arising from exposure to ionizing radiation, whatever the cause. It includes the safety of nuclear installations, radiation safety, the safety of radioactive waste, and safety in transporting radioactive material. It relates to operating conditions, accident prevention, and mitigating the consequences of accidents to protect workers, the public, and the environment from radiation risks.
- **Radiological safety** refers specifically to minimizing the likelihood of exposure involving radioactive sources and, if an accident occurs, mitigating its consequences.

Nuclear and Radiological Facilities in Ukraine

Ukraine has 35 nuclear facilities and other sites that contain nuclear or radioactive material. Before the invasion, Ukraine had 15 operating power reactors at four nuclear power plants, and nuclear power represented 55 percent of its electricity generation.[13] Ukraine's nuclear operator, Energoatom, continues to operate nine reactors across three nuclear power plants (Khmelnitsky, Rivne, and South Ukraine). The Zaporizhzhia Nuclear Power Plant, which has six reactors, is in Russian-controlled territory and is not currently producing energy. Ukraine's reactors are Russian-made and were historically dependent on Russian components and fuels. Ukraine has two research reactors, one each at the Kharkiv Institute of Physics and Technology and Kyiv Institute for Nuclear Research. Ukraine also has facilities with radioactive sources in use and storage, including long-term storage facilities within the Chornobyl Exclusion Zone.

Agency Roles and Responsibilities

NNSA

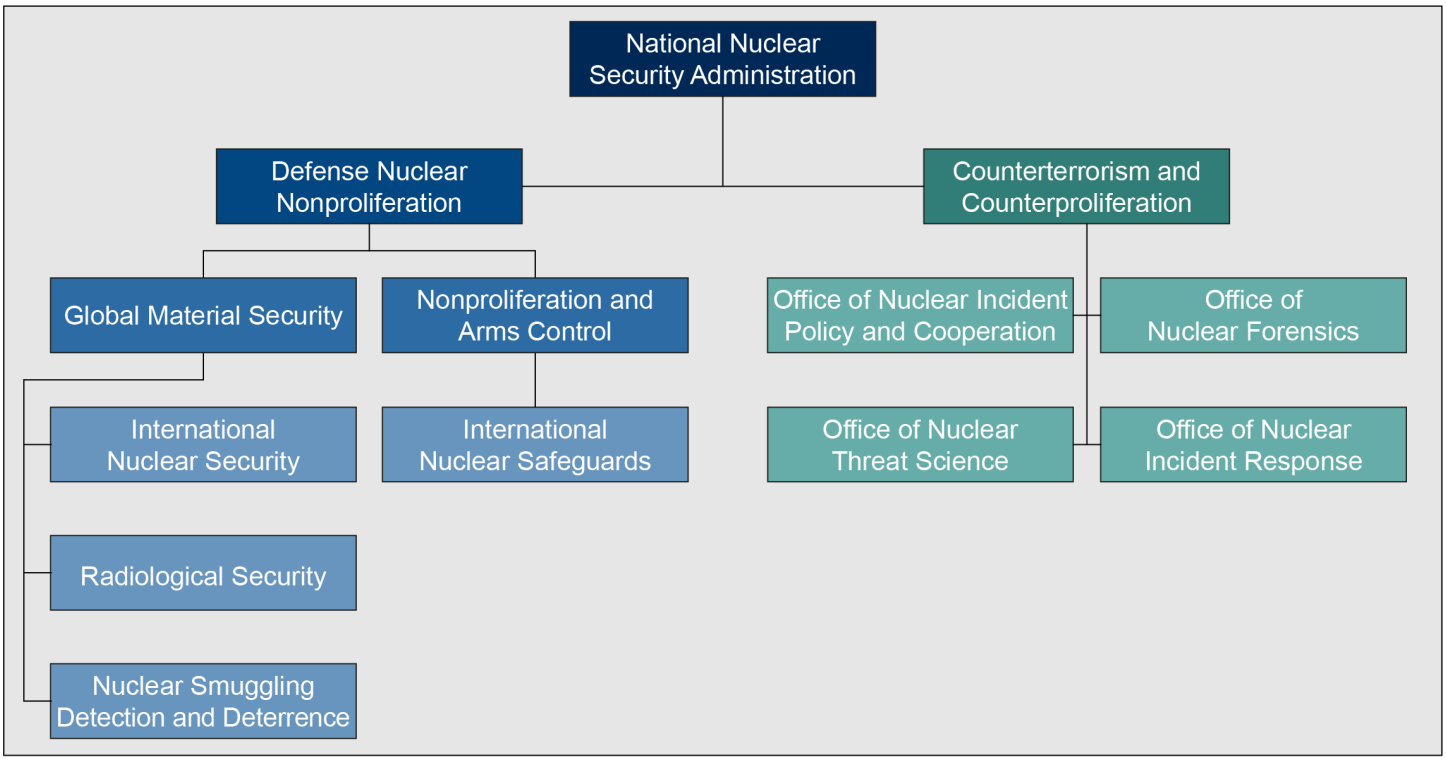
Within NNSA, several offices and their subcomponents are responsible for various aspects of nuclear and radiological security and safety work in or for Ukraine (see fig. 1).

[11]In this report, we use the term "radiation" to refer to ionizing radiation, which includes X-rays, gamma rays, and various types of atomic particles. Ionizing radiation, in high doses, is known to cause cancer and other health effects in humans.

[12]For more information about the potential risks and consequences of radiological dispersal devices, see GAO, *Security of Radioactive Materials*, GAO-22-105498 (Washington, D.C.: Apr. 5, 2022).

[13]Ukraine has a fifth licensed nuclear power plant site at Chornobyl—also known as Chernobyl—at which there are no operating reactors.

Figure 1: National Nuclear Security Administration Offices Responsible for Aspects of Work in Ukraine



Source: GAO. | GAO-25-108444

NNSA, through DNN, works globally to prevent state and nonstate actors from developing nuclear weapons or acquiring weapons-usable nuclear or radioactive materials, equipment, technology, and expertise. DNN includes the following:[14]

- **Office of Global Material Security (GMS)**. This program works with partner countries to improve the security of vulnerable materials and facilities and to build partners' capacity to detect, disrupt, and investigate illicit trafficking of these materials. Subprograms within GMS are
  - the Office of International Nuclear Security, which has the mission of strengthening partner capacity to secure nuclear material;
  - the Office of Radiological Security (ORS), which has the mission to help secure radioactive material worldwide; and
  - the Office of Nuclear Smuggling Detection and Deterrence (NSDD), which establishes radiation detection architecture overseas to detect nuclear and radiological smuggling.
- **Office of Nonproliferation and Arms Control.** This program develops and implements nonproliferation and arms control policy, including management and enforcement of export controls and support of treaty obligations. The Office of International Nuclear Safeguards, within this program, is the primary NNSA

[14]For purposes of discussion in this report, we will refer to the line offices within the Office of Defense Nuclear Nonproliferation as "programs" and the offices within those as "subprograms" (for example, the Office of Nuclear Smuggling Detection and Deterrence is a subprogram of the Global Material Security program).

subprogram supporting the International Atomic Energy Agency (IAEA) and its nuclear safeguards mission.[15]

NNSA also works through its Office of Counterterrorism and Counterproliferation (CTCP) to prepare for nuclear and radiological incidents and develop the technical capability to understand nuclear threats. Subprograms within CTCP include the following:

- The Office of Nuclear Incident Policy and Cooperation provides capacity-building emergency preparedness training to counter and respond to radiological and nuclear incidents, accidents, and terror threats.
- The Office of Nuclear Threat Science develops scientific knowledge of nuclear and radiological threat devices.
- The Office of Nuclear Forensics sustains nuclear forensics personnel, equipment, facilities, and operations. Nuclear forensics are used to determine the origin of nuclear materials outside of regulatory control, such as those seized from nuclear smugglers, and to support attribution of responsibility in the event of an attack.
- The Office of Nuclear Incident Response manages the Nuclear Emergency Support Team. This team of scientific and technical experts is trained and equipped to respond rapidly to nuclear or radiological incidents and accidents worldwide. This subprogram also supports international partners' capacity to respond effectively to nuclear or radiological incidents in their countries.

DOE and NNSA Contractors

DOE and NNSA rely on contractors to execute most of their work. DOE and NNSA use management and operating (M&O) contracts to manage and operate national laboratories and other sites.[16] The agencies also use other contract types such as "indefinite delivery, indefinite quantity" (IDIQ) contracts.[17] DOE's and NNSA's contracting activities are governed by federal law and regulations, including the Federal Acquisition Regulation (FAR) as supplemented by the Department of Energy Acquisition Regulation.[18]

For the purposes of this report, a contractor is a party that has signed a contract with DOE (known as a prime contract), while a subcontractor is a party that has signed a contract with a DOE contractor (or another subcontractor). We have previously found weaknesses in DOE's oversight of subcontractors,[19] and there have been allegations of fraudulent activity involving DOE subcontracts. For example, in 2021, a DOE prime

[15]IAEA is an autonomous international organization affiliated with the United Nations and based in Vienna, Austria. The agency was founded with the dual mission of (1) promoting the peaceful uses of nuclear energy by transferring nuclear science and technology through its nuclear science and applications and technical cooperation programs, and (2) verifying, through its safeguards program, that nuclear material subject to safeguards is not diverted to nuclear weapons or other proscribed purposes. IAEA has taken on other roles and established other programs, including its Department of Nuclear Safety and Security.

[16]A M&O contract is an agreement under which the government contracts for the operation, maintenance, or support, on its behalf, of a government-owned or -controlled research, development, special production, or testing establishment wholly or principally devoted to one or more major programs of the contracting federal agency. 48 C.F.R. § 17.601.

[17]An IDIQ contract provides for an indefinite quantity, within stated limits, of supplies or services during a fixed period.

[18]The FAR is the primary regulation for executive agencies in their acquisition of supplies and services.

[19]GAO, *Department of Energy Contracting: Actions Needed to Strengthen Subcontract Oversight*, GAO-19-107 (Washington, D.C.: Mar. 12, 2019).

contractor settled to resolve allegations that it violated the False Claims Act by submitting false and fraudulent small business subcontract reports. In an internal fiscal year 2024 risk assessment, DOE identified the potential for fraud and improper payments in contracts as a top risk, in part as a function of increased contract amounts resulting from supplemental funding.

Other Agencies

In addition to NNSA, the following federal agencies have various roles in supporting international nuclear and radiological security and safety, including in Ukraine:

- **Department of State.** State's Bureau of International Security and Nonproliferation implements a range of nonproliferation policies and assistance programs related to nuclear security and safety. State is also the lead agency for coordinating U.S. policy with, and financial contributions to, IAEA.
- **Nuclear Regulatory Commission.** The NRC regulates commercial nuclear power plants and other uses of nuclear materials in the United States, such as in nuclear medicine, through licensing, inspection, and enforcement of its requirements, including safety and security. NRC's international assistance program seeks to enhance foreign regulatory counterparts' ability to safely and securely regulate their nations' civilian nuclear power programs and use of radioactive material. Historically, NRC has provided training and assistance to Ukraine's nuclear regulatory agency as Ukraine established relevant laws, regulations, and expertise. NRC also regularly participates in IAEA activities to enhance global nuclear safety and security.
- **Department of Defense.** DOD's Cooperative Threat Reduction Program's mission includes the prevention of the proliferation or use of weapons of mass destruction (WMD) by working with partner nations to secure, eliminate, detect, and interdict WMD-related systems and materials. This program's Global Nuclear Security subprogram transports fissile and radiological materials from less secure to more secure sites and disposes of them. It also builds partner nations' capacity to counter nuclear smuggling and secure nuclear weapons, nuclear weapons materials, nuclear weapons components, high-threat radiological material, and related items.

  Since Russia's 2022 invasion of Ukraine, DOE and NNSA have coordinated with these and other federal agencies on efforts to support nuclear and radiological security and safety in Ukraine. Coordination mechanisms include weekly phone calls and regular interagency coordination meetings, and the Ukraine Task Force, which NNSA established. According to the task force's charter, its purpose is to

  - integrate, coordinate, and formalize efforts to reduce the nuclear risks associated with the war, respond to emerging needs, and support Ukraine's recovery after the war; and
  - serve as an integrated point of contact on Ukraine-related nuclear issues for other elements of DOE, other federal agencies, and international bilateral and multilateral partners.

In addition to these federal agencies, IAEA, an autonomous international organization, identifies and promotes best practices, safety standards, and security guidelines through its Department of Nuclear Safety and Security. This department also implements programs to help countries apply these standards. IAEA's

Department of Safeguards carries out technical measures and activities to verify that nuclear material subject to safeguards is not diverted to nuclear weapons or other proscribed purposes.[20]

Federal and DOE Fraud Risk Management Requirements, Guidance, and Best Practices

Various sets of requirements, guidance, and best practices govern agencies in establishing controls to manage fraud risk in their programs and activities. Specifically, GAO's Fraud Risk Framework describes leading practices to prevent, detect, and respond to fraud, emphasizing prevention and environmental factors that help managers mitigate fraud risks in their programs.[21]

Federal and departmental guidance and requirements cite the Fraud Risk Framework:

- OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, states that agencies should adhere to the framework's leading practices as part of their efforts to effectively design, implement, and operate an internal control system that addresses financial and nonfinancial fraud risks.
- OMB Controller Alert 23-03 reminds agencies to adhere to leading practices in the Fraud Risk Framework to assess fraud risk, including risks that do not rise to the level of enterprise-wide risks.[22]

  DOE's Enterprise Risk Management (ERM) guidelines, established by its Office of the Chief Financial Officer, provide department-wide guidance on risk assessment, including for fraud risk. DOE implements GAO's Fraud Risk Framework through this guidance. The guidance directs DOE entities, including NNSA, to assess fraud risk for each fiscal year as part of an annual risk assessment cycle.[23]

[20]The U.S. is the largest contributor to IAEA's regular budget.

[21]GAO-15-593SP.

[22]Office of Management and Budget, *Establishing Financial and Administrative Controls to Identify and Assess Fraud Risk*, Controller Alert 23-03 (Oct. 17, 2022).

[23]NNSA is also subject to the FAR and the Department of Energy Acquisition Regulation, which may support fraud risk management in contracts.

NNSA and Other Key Agencies Intensified Support for Nuclear and Radiological Security and Safety in Ukraine After the 2022 Invasion

NNSA and other key agencies supported a range of nuclear and radiological security and safety efforts in Ukraine for decades before the 2022 invasion. These agencies expanded that support in response to the invasion. NNSA used its supplemental funding to broaden and intensify its efforts. State and NRC used a mix of supplemental and regular funding to enhance or refocus their efforts, while DOD used regular funding.

Before the 2022 Invasion, NNSA and Other Agencies' Support to Ukraine Included Facility Security Upgrades, Training, and Radiation Detection

NNSA has a long history of supporting nuclear and radiological safety and security in Ukraine. In the years before the 2022 invasion, NNSA's GMS program spent less than $30 million per year on activities in or with Ukraine. For example, from fiscal years 2017 through 2022, GMS obligated between $14.2 million and $27.0 million annually across three subprograms (see table 1).

Table 1: NNSA Office of Global Material Security (GMS) Expenditures to Support Nuclear and Radiological Security and Safety for Ukraine, Fiscal Years (FY) 2017–2022

(Dollars in millions)

GMS office	FY17	FY18	FY19	FY20	FY21	FY22
International Nuclear Security	$4.5	$4.7	$0.8	$3.8	$2.1	$2.1
Radiological Security	$3.2	$3.2	$4.1	$2.5	$4.5	$3.3
Nuclear Smuggling Detection and Deterrence (NSDD)[a]	$16.3	$8.7	$9.2	$11.2	$9.9	$21.6
Total	**$24.0**	**$16.6**	**$14.2**	**$17.5**	**$16.5**	**$27.0**

Source: GAO analysis of National Nuclear Security Administration (NNSA) data. | GAO-25-108444

Note: Amounts may not total because of rounding.

[a]A portion of the NSDD expenditures represent equipment that was procured in prior years or with non-Ukraine specific funds.

GMS subprograms supported various efforts during this time frame. For example:

- the Office of International Nuclear Security provided physical protection upgrades at facilities with nuclear materials and cybersecurity training for Ukrainian nuclear power plant operators;
- the Office of Radiological Security inventoried and mapped locations of Ukraine's facilities with high-activity radioactive sources. This office also supported physical security upgrades at 83 buildings with radioactive materials, consolidation and secure storage of disused sources from 11 sites, and replacement of sources with alternative technologies at three sites;[24] and
- the Office of Nuclear Smuggling Detection and Deterrence installed radiation detection systems to detect nuclear smuggling at about 90 official points of entry and deployed 18 mobile radiation detection systems (see fig. 2).

[24]A disused source is a radioactive source that is no longer used, and is not intended to be used, for the purpose for which it was licensed. It may still represent a significant radiological hazard.

Figure 2: Radiation Portal Monitors Provided by NNSA's Nuclear Smuggling Detection and Deterrence Program

Source: National Nuclear Security Administration (NNSA). | GAO-25-108444

Other NNSA offices did not specifically support nuclear security or safety in Ukraine before the invasion. For example, before February 2022, the Office of Nonproliferation and Arms Control, which broadly supports IAEA's Safeguards program, did not specifically support IAEA efforts in Ukraine. The Office of Counterterrorism and Counterproliferation, which focuses on emergency preparedness and response, also did not operate routine programs in Ukraine.

State, DOD, and NRC also operated nuclear security and safety programs in Ukraine before the 2022 invasion, often in coordination with NNSA:

- **State.** The Bureau of International Security and Nonproliferation (ISN) has used funding from its Nonproliferation and Disarmament Fund to support nuclear and radiological security and safety efforts in Ukraine. These funds, which are available until expended, support the rapid response to unanticipated or unusually difficult, high priority circumstances around the world.[25] Since Russia's 2014 invasion of Crimea, ISN has used this funding for various efforts, including $630,000 to help Ukrainian government agencies identify abandoned and loose nuclear and radiological materials near the conflict zones.[26] ISN has also provided border security equipment to Ukrainian partners and supported Ukraine's counter-trafficking capabilities.

[25]Appropriated funds that remain available indefinitely are commonly referred to as "no-year" funds. State officials described the Nonproliferation and Disarmament Fund as the U.S. government's contingency fund for chemical, biological, nuclear, radiological, and high-yield explosives threats. The fund is designed to allow flexibility to fill gaps or meet immediate needs before other offices can act. Officials may use various authorities to draw down from the fund to address such threats as they emerge.

[26]In 2014, Russia also took control of parts of the Donetsk and Luhansk regions of eastern Ukraine (the Donbas), which have been sites of conflict.

- **DOD.** DOD has provided nuclear and radiological security assistance to Ukraine through the Cooperative Threat Reduction program.[27] Before the 2022 invasion, this program's nuclear and radiological security work in Ukraine focused on the capacity building of institutions. DOD obligated a total of $6.7 million in fiscal years 2020 and 2021 for this assistance through its Global Nuclear Security subprogram.[28]
- **NRC.** NRC's support for nuclear security and safety in Ukraine before the 2022 invasion generally focused on the exchange of information on regulatory matters, including physical protection. NRC officials told us that these activities were coordinated on the basis of a biennial "memorandum of meeting" with Ukraine's nuclear regulatory agency.[29] Under this memorandum, NRC and Ukraine's regulator and technical support organization have shared information, held bilateral meetings, and hosted workshops to exchange regulatory insight about a range of nuclear safety and security issues, such as licensing and reactor oversight, probabilistic risk assessments, risk-informed regulation, and insider threats.[30] Before the 2022 invasion, NRC spent less than $100,000 per year on these activities.

Since the 2022 Invasion, NNSA Has Used Supplemental Funding to Expand Existing Efforts and Initiate New Efforts Related to Nuclear Emergency Preparedness and Response

NNSA has used the funding it received from Ukraine supplemental appropriations acts to expand existing efforts and initiate new efforts to address nuclear and radiological security and safety risks in Ukraine resulting from the 2022 invasion and ongoing conflict. These risks include damage and destruction of facilities housing nuclear and radioactive material, loss of regulatory control over nuclear and radiological facilities in occupied areas, and security and safety challenges at nuclear power plants, according to our review of NNSA and IAEA documents, unclassified interviews with NNSA officials, and written responses from Ukrainian agencies.[31]

NNSA's overall response to the invasion has focused on preparing for, preventing, and minimizing the consequences of nuclear and radiological incidents, according to NNSA documents. NNSA has used the

[27]The Cooperative Threat Reduction program comprises several subprograms, including Global Nuclear Security, the Proliferation Prevention Program, and subprograms focused on chemical and biological threats. Three DOD entities manage the Cooperative Threat Reduction program, including the Defense Threat Reduction Agency. This agency, which focuses on addressing the threats posed by weapons of mass destruction, executes the program's activities.

[28]These amounts reflect funds that were obligated to the Global Nuclear Security subprogram. DOD documents include other amounts (for example, $3.5 million and $1.95 million appropriated for the subprogram's work in Ukraine for fiscal years 2020 and 2021, respectively). No such document exists for fiscal year 2022, and DOD documents show no funds requested for Global Nuclear Security work that year.

[29]NRC officials told us that NRC and Ukraine's nuclear regulatory agency signed the most recent "memorandum of meeting" in 2023. NRC also has an agreement with the State Nuclear Regulatory Inspectorate of Ukraine that serves as a mechanism to share nonpublic information. See Nuclear Regulatory Commission, *Arrangement with the State Nuclear Regulatory Inspectorate of Ukraine for the Exchange of Technical Information and Cooperation in Nuclear Safety Matters*, Ukraine (23-801) (signed at Rockville on July 10, 2023, and Kyiv on August 1, 2023).

[30]In light of the COVID-19 public health emergency, NRC largely supported Ukraine's regulator from fiscal years 2020 to 2022 virtually. The support, generally provided through Brookhaven National Laboratory, related to computer codes, system analyses, and regulatory requirements.

[31]The CUI report and classified annex accompanying this report provides more detail about the nuclear power plant safety risks and other nuclear and radiological security and safety risks. See GAO-25-107015SU and GAO-25-107768C.

$161.3 million in funding it received through the Ukraine supplemental appropriations acts for its efforts. Table 2 shows how NNSA allotted these funds to its offices and associated programs.

Table 2: NNSA's Allotment of Supplemental Appropriations Acts Funding by Program

(Dollars in millions)

Program	Allotment
Global Material Security	$49.0
Nonproliferation and Arms Control	$2.0
Counterterrorism and Counterproliferation	$110.3
Total	**$161.3**

Source: National Nuclear Security Administration (NNSA). | GAO-25-108444

Note: An allotment is an authorization by either the agency head or another authorized employee to their subordinates to incur obligations within a specified amount. An obligation is a definite commitment that creates a legal liability of the government for the payment of goods and services ordered or received, or a legal duty on the part of the United States that could mature into a legal liability by virtue of actions on the part of the other party beyond the control of the United States. GAO, *A Glossary of Terms Used in the Federal Budget Process* (Supersedes AFMD-2.1.1), GAO-05-734SP (Washington, D.C.: Sept. 1, 2005).

Expanded Efforts

NNSA used its supplemental funding to expand or adapt the nuclear and radiological security and safety efforts GMS had been conducting in Ukraine prior to the 2022 invasion, such as providing radiation detection equipment to counter nuclear smuggling. Table 3 provides examples of efforts that GMS executed using supplemental funding.

Table 3: Examples of Expanded Nuclear and Radiological Security and Safety Efforts Led by NNSA's Global Material Security (GMS) Program in Ukraine, by Subprogram

GMS subprogram	Example of efforts
International Nuclear Security	Supporting repairs and upgrades—such as to mitigate potential sabotage—at nuclear power plants under Ukrainian control and additional cybersecurity training and equipment to plant operators. Supporting the delivery of emergency diesel generators to nuclear power plants under Ukrainian control.
Office of Radiological Security	Supporting physical security and monitoring of buildings housing radioactive material for damage from ongoing military action and to mitigate compromised data transmission capabilities that resulted from the invasion. Such monitoring provides information about potential material vulnerability. Procuring equipment and vehicles to remove disused radioactive sources and protect those that must remain in place, in response to identified threats that include damage and destruction to facilities housing such material and loss of regulatory control over radiological facilities in occupied areas.
Nuclear Smuggling Detection and Deterrence	Supporting efforts to sustain and salvage radiation portal monitors for Ukraine's border guards throughout the country to help detect any incidents of nuclear or radiological smuggling. Deploying radiation portal monitors for Ukrainian border guards at new border crossing points. Procuring handheld and other mobile radiation detection units for Ukraine's Emergency Services, National Guard, and National Police. Providing equipment and training to Ukraine's State Security Service, which would be responsible for investigating any internal detections or reports of illicit movement of nuclear or radioactive material.

Source: GAO analysis of information from the National Nuclear Security Administration (NNSA) and Government of Ukraine. | GAO-25-108444

New Efforts

After the 2022 invasion, NNSA also used its supplemental funding to initiate new programmatic efforts. As noted above, most of the $161.3 million in supplemental funding was allotted to CTCP, which used the funding to support several major new efforts:

- establishing training for teams specialized in nuclear incident response in Ukraine;
- establishing remote sensing capabilities to acquire data on potential nuclear and radiological incidents in and around Ukraine; and
- acquiring new high-performance computing capabilities at U.S. national laboratories

CTCP also worked with GMS's Office of International Nuclear Security to provide emergency diesel generators for nuclear power plants to help prevent a nuclear safety incident. Diesel generators provide backup power for cooling and operating power plant systems.

The Office of Nonproliferation and Arms Control allotted $2 million in supplemental funding to support IAEA efforts in Ukraine.

Other Agencies Used Regular and Supplemental Funding to Support Nuclear and Radiological Security and Safety in Ukraine

State, NRC, and DOD intensified their efforts using funding from their regular annual appropriations acts and Ukraine supplemental appropriations acts. In addition, IAEA established a joint mission in Ukraine, with support from U.S. agencies and other member states. Table 4 shows the amount of funding each agency obligated for efforts to support nuclear and radiological security and safety in Ukraine in 2022 and 2023.

Table 4: Other U.S. Agencies' Obligations to Support Ukraine Nuclear and Radiological Security and Safety from February 2022 Through December 2023

(Dollars in millions)

Agency	Total obligations	Obligations from supplemental appropriations	Obligations from regular appropriations
Department of State[a]	**$54.0**	$16.8	$37.2
Nuclear Regulatory Commission[b]	**$1.3**	$0.8	$0.5
Department of Defense	**$44.9**	$0	$44.9
Total	**$ 100.2**	**$17.6**	**$82.6**

Source: GAO analysis of agency data. | GAO-25-108444

[a]State's obligations include some expenditures for equipment to counter a range of chemical, biological, nuclear, and radiological threats in the region.

[b]This table covers funding obligated following the 2022 invasion through the end of calendar year 2023, including from the Ukraine supplemental appropriations acts. Some funds were obligated from prior-year or regular appropriations. In addition to the obligations shown above, the Nuclear Regulatory Commission had also obligated $955,000 from the Ukraine supplemental appropriations acts as of October 2024.

State. In 2022 and 2023, State obligated funding from Ukraine supplemental appropriations and regular annual appropriations to address nuclear and radiological security and safety risks in Ukraine. State support included the following:

- State obligated $15 million that the Nonproliferation and Disarmament Fund received from supplemental appropriations for nuclear-related disaster relief support to Ukraine's emergency services. This support included providing radiation detection and decontamination equipment for Ukrainian responders.[32] The $15 million was part of $43.7 million obligated for material assistance to support and outfit first responders and security forces in Ukraine.
- The Office of WMD Terrorism obligated $1.8 million from supplemental appropriations to, among other things, support Ukrainian partners in securing radiological and nuclear materials and facilities, including the Chornobyl Exclusion Zone, as well as providing personal protective equipment, individual dosimeters, the restoration of automatic radiation monitoring systems, and other radiation detection equipment.
- The Office of Multilateral Nuclear and Security Affairs obligated $8 million from regular appropriations to support IAEA's work in Ukraine.

DOD. DOD used funding from regular appropriations acts to support its nuclear and radiological security and safety efforts in Ukraine.[33] Specifically, DOD's Global Nuclear Security program obligated $44.9 million between February 2022 and December 2023 to provide radiological, nuclear, and chemical response equipment and capabilities to various agencies in Ukraine. This included funds to increase Ukraine's capability to secure fissile and radiological material in the country and to counter nuclear smuggling and illicit trafficking throughout Ukraine and the region.

NRC. NRC received $2 million in Ukraine supplemental appropriations to provide regulatory and technical support. Of this amount, NRC obligated $832,000 in 2022 and 2023 for nuclear safety modeling. Specifically, NRC provided technical assistance to Ukraine's nuclear regulatory authority to support modeling of how U.S.-designed nuclear fuels would perform in Ukraine's nuclear reactors, to reduce Ukraine's dependence on Russian fuel. NRC also used some of the funding to support modernizing Ukraine's radiological source registry and provide cybersecurity training to, among other things, help detect malware.[34] NRC officials told us that they also obligated $500,000 in 2022 from prior-year regular appropriations to IAEA's Response and Assistance Network (RANET).[35] IAEA has used this funding to deliver equipment, such as laptops and power supply systems, for Ukraine. According to NRC officials, some of this equipment helped Ukrainian nuclear regulatory staff continue working during the conflict.

IAEA. In addition to these U.S. agency efforts, IAEA established a joint nuclear safety, security, and safeguards mission in Ukraine, which receives support from DOE, NRC, and State, as well as contributions

[32]Much of the personal protective and decontamination equipment provided by the Nonproliferation and Disarmament Fund is for a range of uses, including to protect against chemical and biological agents as well as nuclear and radiological material. Certain sensors it provided, such as personal radiation detectors and dosimeters, are radiological- and nuclear-specific.

[33]As noted above, the Ukraine supplemental appropriations acts did not provide DOD funding for its nuclear and radiological security and safety efforts in Ukraine.

[34]NRC obligated another $955,000 of this amount in 2024 for equipment to move Ukraine's nuclear regulatory staff to a more protective building.

[35]RANET is an IAEA network for pooling assistance from member states to those that request such assistance.

from other member States.[36] IAEA officials told us that after the conflict started in 2022, IAEA implemented in-person missions to better understand the impact of the conflict, the resulting needs, and how to best support Ukraine. The agency complements its continuous presence with ad hoc missions, as needed. IAEA's efforts include the following, according to IAEA documents and officials:

- Reporting on the challenges of implementing safeguards in conflict zones, as well as a range of nuclear security and safety risks, particularly at the Russian-controlled Zaporizhzhia Nuclear Power Plant.
- Helping to identify equipment affected by the conflict and delivering needed equipment to Ukraine. Since the start of the conflict, IAEA has arranged 84 deliveries to 23 different agencies in Ukraine in shipments worth a total of more than $14.5 million. These include in-kind contributions from member states as well as equipment that IAEA procured. IAEA uses RANET to coordinate this assistance.[37] Member states send direct contribution offers through RANET and its established network.
- Working with plant operating staff to gauge the stressors on personnel and impacts of the war on them and their families. Plant operators under duress, and the resulting increased risk of human error, can contribute to continued risks to nuclear safety and security, IAEA officials told us.

NNSA Did Not Conduct a Fraud Risk Assessment for Its Ukraine-Related Efforts, but NNSA and Its Contractors Took Steps to Mitigate Fraud Risks at the Contract Level

DOE's Enterprise Risk Management (ERM) guidance directs its offices to annually assess risks, including fraud risk, consistent with the leading practices in GAO's Fraud Risk Framework.[38] However, this guidance does not include a key leading practice to assess risk when a program experiences structural change, a change in its operating environment, or adds new services. This practice helps to ensure that fraud risk assessments are relevant, iterative, and timed based on need. In following DOE guidance, NNSA did not conduct a fraud risk assessment tailored to its nuclear and radiological security and safety efforts in Ukraine, although NNSA took steps to manage fraud risk for individual contracts.

NNSA assesses fraud risks as part of DOE's annual ERM cycle, in accordance with departmental ERM guidance.[39] Through this process, NNSA develops a risk profile that identifies the top risks the agency faces, including fraud risks.[40] However, according to the Fraud Risk Framework, structural changes to a program, changes to the operating environment, or the addition of new services can warrant more frequent risk assessments than the regularly planned intervals in which an agency normally assesses risk. Agencies should plan and conduct fraud risk assessments tailored to a program before designing and implementing an antifraud

[36]Before the invasion, IAEA was conducting these as three separate missions.

[37]IAEA first received requests from Ukraine to RANET in April 2022 for nuclear safety and security equipment, according to IAEA officials.

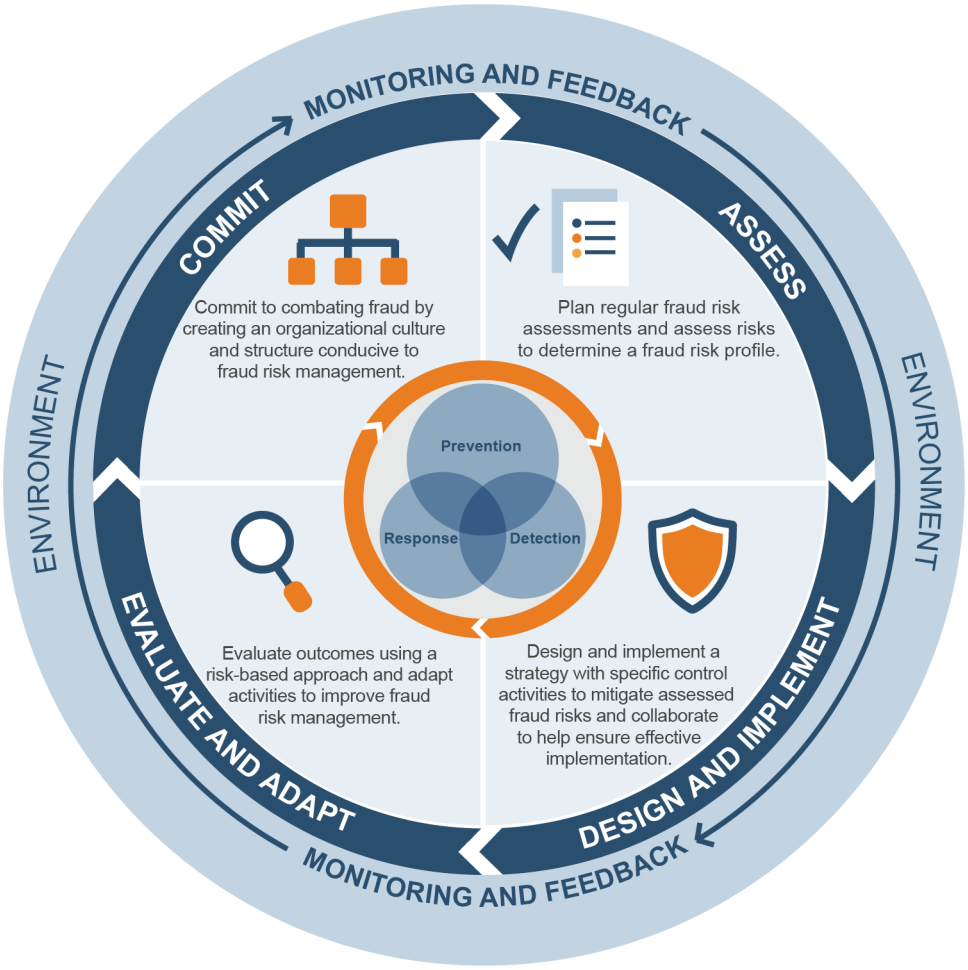
[38]DOE's ERM contains fraud risk management direction to internal components it refers to as "reporting organizations." In this report we refer to these as offices.

[39]NNSA and M&O contractors complete this process from December through early February each year.

[40]NNSA's and other DOE offices' risk profiles feed into a consolidated risk profile for DOE as a whole.

strategy that includes specific controls designed to mitigate fraud risks, according to the framework (see fig. 3).[41] This provides for a more strategic, risk-based approach to managing fraud risks and developing effective antifraud controls, according to the framework.

Figure 3: GAO's Fraud Risk Management Framework



Source: GAO. | GAO-25-108444

Note: The Fraud Risk Framework identifies a series of overarching concepts and leading practices for fraud risk management and conceptualizes those practices into a risk-based framework to aid program managers in managing fraud risks. GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 2015).

The operating environment in which NNSA has executed its Ukraine-related efforts changed significantly after Russia's 2022 invasion. As described above, the federal government's response to this invasion triggered

[41]The Fraud Risk Framework identifies a series of "overarching concepts" and leading practices for fraud risk management and conceptualizes those practices into a risk-based framework to aid program managers in managing fraud risks. See GAO-15-593SP. The Office of Management and Budget (OMB) must maintain guidelines for agencies to establish financial and administrative controls to identify and assess fraud risks, incorporating leading practices detailed in the framework. 31 U.S.C. § 3357(b).

NNSA's expansion of ongoing programmatic efforts and initiation of new programmatic efforts. The changes to the operating environment include the following:

- A security environment in Ukraine that limits NNSA's ability to verify in person that equipment is delivered and working.
- Provision of assistance in an active conflict zone, which heightens risk for diversion of assistance through fraud and corruption.
- Rapid execution of funding to address immediate needs in Ukraine and to meet spending deadlines. For example, NNSA had less than 3 months to obligate funds from the first continuing resolution in fiscal year 2023.[42]

Furthermore, NNSA added several new efforts to support Ukraine in 2022, such as those implemented by the Office of Counterterrorism and Counterproliferation, which did not previously operate programs in the country, according to officials.

However, NNSA did not conduct a fraud risk assessment tailored to its programmatic efforts in Ukraine, according to NNSA officials. These officials noted two reasons for not assessing fraud risk facing this program:

- DOE's ERM guidance does not contain specific direction for when programs should reassess fraud risk; and
- the contractors that executed most of the funds had ultimate responsibility for fraud risk management, often through subcontract oversight (see app. II for a summary of the steps NNSA contracting officers and contractor representatives in our sample took to mitigate fraud risk and oversee subcontracts).

DOE's ERM guidance directs offices to adhere to the leading practices in the Fraud Risk Framework, but it does not contain specific direction about planning to conduct assessments when changes occur, according to our review of the guidance. Specifically, the guidance does not advise offices to consider whether the addition of new services or changes to a program's operating environment warrant a program-level fraud risk assessment outside of the annual higher-level, agencywide risk assessments.[43] As we previously reported, DOE offices may perform additional tasks beyond the ERM minimum requirements to identify and assess fraud risks as part of their internal control processes.[44] The Fraud Risk Framework notes that the frequency of fraud risk assessments is a function of need and not just a matter of demonstrating compliance with standards.

DOE's ERM guidance directs offices to consider factors such as significant budget increases and policy or legislative changes during their annual, higher-level risk assessments. Officials with DOE's Office of the Chief Financial Officer, which is responsible for DOE's ERM process, said this guidance applies to programs receiving supplemental funds, such as those supporting NNSA's Ukraine efforts. However, while the ERM guidance specifically identifies risk considerations for certain acts that heightened fraud risk due to increased

[42]The Continuing Appropriations Act, 2023 became law on September 30, 2022. The act required NNSA to obligate funds by December 16, 2022.

[43]Department of Energy, *Enterprise Risk Management Fiscal Year 2024 Guidance* (December 2023).

[44]GAO, *Improvements Needed to Ensure DOE Assesses Its Full Range of Contracting Fraud Risks*, GAO-21-44 (Washington, D.C.: Jan. 13, 2021).

funding for DOE activities, such as the Infrastructure Investment and Jobs Act and the CHIPS and Science Act, it does not include the Ukraine supplementals in this list.[45]

NNSA officials and representatives of M&O contractors might not have interpreted this guidance as applicable to the Ukraine supplemental appropriations acts, according to officials with the Office of Financial Performance, the NNSA office responsible for ensuring the agency follows DOE's ERM requirements. Specifically, they said these officials and contractors might not have viewed the $161.3 million in total supplemental funding appropriated to NNSA as a significant increase because the funds were divided among multiple contractors that consistently manage billions of dollars annually.[46] Officials from the Office of Financial Performance said that while they would not direct a DOE entity to assess program-specific fraud risk beyond the annual requirement in DOE's ERM guidance, these entities can proactively assess fraud risk beyond that requirement.

Example of Contract-Level Fraud Risk Management in Ukraine Contracts: Radiation Detection Equipment

The National Nuclear Security Administration (NNSA) used an existing cost reimbursement contract to provide radiation detectors to Ukraine.

Cost-reimbursement contracts have a higher risk of cost variance than firm fixed-price contracts. NNSA documented its choice to use this contract structure in a risk assessment.

The assessment identified several risks, including the unpredictability of the situation in Ukraine limiting NNSA's ability to accurately estimate costs and deadlines to spend supplemental funds. The assessment noted NNSA's willingness to tolerate certain risks to meet the deadline and meet critical needs.

NNSA also assessed its existing controls for this contract, which it had already enhanced following a 2016 program review of the contract, and determined they were sufficient to mitigate the identified risks. NNSA officials told us that the controls include requiring proof for every purchase, rather than only those exceeding a certain price, and requiring a monthly report to track variance between actual and estimated costs.

Source: NNSA documents and interviews and Federal Acquisition Regulation. | GAO-25-108444

Separately from its overall risk assessment process, based on our review of selected contracts, NNSA and its contractors took varying approaches to assess and manage fraud risk at the contract level. NNSA provided nuclear and radiological security and safety assistance for Ukraine through multiple contracts. NNSA oversaw one of these contracts directly, while other contractors—mainly DOE's and NNSA's M&O contractors—managed the others as prime contractors and issued subcontracts. NNSA's fiscal year 2024 risk profile identified the following as at risk for fraud: contractor oversight, procurement, labor charging practices, and property management.[47]

We reviewed a sample of eight of NNSA's largest contracts funded using Ukraine supplemental appropriations acts and that involved the use of subcontractors. In some cases, NNSA contracting officers and prime contractor officials told us and provided documentation showing that they assessed fraud risk for the subcontracts funded through these contracts. They used these assessments to test their existing fraud controls. For example, an NNSA contracting officer's representative overseeing a cost-reimbursement contract—a contract structure with inherently higher risk for cost variance than a firm fixed-price contract—took

[45]Infrastructure Investment and Jobs Act, Pub. L. No. 117-57, 135 Stat. 429 (2021); CHIPS Act of 2022, Pub. L. No. 117-167, div. A, 136 Stat. 1372 (this law is also known as the CHIPS and Science Act). "CHIPS" stands for "Creating Helpful Incentives to Produce Semiconductors."

[46]That is, no single contractor received a significant funding increase in comparison to the level of funding they normally execute, according to the officials.

[47]According to the risk profile, NNSA took steps to mitigate these risks, including comparing M&O practices against GAO's Fraud Risk Framework, which resulted in low residual fraud risk for NNSA.

additional steps to assess fraud risks for work conducted in Ukraine.[48] These steps included assessing the suitability of NNSA's existing fraud control processes (see sidebar).

In other cases, prime contractor officials told us that they did not conduct such assessments before executing funds. NNSA officials and prime contractor representatives for a fixed-price contract said they did not take additional steps to assess fraud risk beyond routine contracting assurances because the contract was to purchase equipment that would

Example of Contract-Level Fraud Risk Management in Ukraine Contracts: Radiological Site Security

The contractor for the Pacific Northwest National Laboratory (PNNL) used a firm fixed-price subcontract to support activities related to monitoring radiological site security. These activities included technical assistance, physical protection for sites with high-activity sources, and transportation security for radiological sources.

PNNL contractor representatives said they vetted subcontractors for financial and technical responsibility. They also managed payments through an approved purchasing system.

PNNL's site office also asked the contractor to notify it of any contracting actions, such as awarding new or modifying existing subcontracts, along with an explanation of the action's impact on Ukraine and NNSA's mission.

Source: NNSA documents and interview. | GAO-25-108444

be tested and installed in the United States before issuing any payments. Such fixed-price contracts have lower risk for cost variance.[49]

Some NNSA contracting officers and contractor representatives also described various actions they took that were intended to mitigate fraud risks and provide subcontract oversight, even if an underlying fraud risk assessment was not conducted for those contracts. Some of these actions included

- requesting photos or videos to verify that the equipment had reached the end user and was operational, since NNSA officials could not verify in person because of the war;
- coordinating with NNSA program staff and contracting officers to verify that subcontractors' purchases aligned with needs on the ground, according to NNSA officials; and
- verifying subcontractor capabilities before awarding funds.

[48]Under cost-reimbursement contracts, the government reimburses a contractor for allowable costs incurred, to the extent prescribed by the contract. Cost-reimbursement contracts can be used when uncertainties involved in contract performance do not permit costs to be estimated with sufficient accuracy to use a fixed-price contract. This type of contract involves high risk for the government because of the potential for cost escalation and because the government pays a contractor's costs of performance regardless of whether the work is completed.

[49]Under fixed-price contracts, the government and contractor agree on a firm pricing arrangement that is subject to adjustment only according to the terms of the contract, and the contractor generally must deliver the product or service for that price.

NNSA contracting officers and contractor representatives told us they based their approaches and design of contract-level fraud risk controls on requirements in the FAR, DOE Acquisition Regulations, and other NNSA internal guidance. For example, the consent review performed by NNSA officials for one of the M&O contractor's subcontracts is a FAR requirement, while the subcontractor vetting performed by another M&O contractor was based on a DOE quality assurance order.[50]

Example of Contract-Level Fraud Risk Management in Ukraine Contracts: Mobile Diesel Generators

The contractor for the Argonne National Laboratory (ANL) issued a subcontract to provide mobile diesel generators as sources of emergency backup power for Ukrainian nuclear power plants.

ANL officials conducted pre-award vetting on vendor capability commensurate with the dollar value and importance of the work, which is an acquisition policy detailed in ANL's Procurement Operations Manual.

In line with this guidance, an ANL official visited the subcontractor's facility to ensure it had the capability to perform the contracted work. ANL requested photos and certificates of assembly to verify equipment reached its destination and was installed properly.

Source: NNSA documents and interviews (text). | GAO-25-108444

However, without a program-level assessment, it is unclear whether the fraud mitigation controls that NNSA and its contractors used were sufficient given the changed operating environment and the new services introduced. By conducting a program-level assessment, NNSA and its contractors could have more systematically analyzed these risks at a programmatic level and better ensured their controls were adequate to address the changed operating environment resulting from the invasion of Ukraine and the influx of $161.3 million in supplemental funding.

By updating its ERM guidance to direct offices and program managers to consider whether the addition of new services or changes to a program's operating environment warrant a fraud risk assessment, DOE will better ensure its offices assess and mitigate emerging fraud risks in programs that have had structural changes outside of DOE's regular risk assessment cycle.

NNSA Transitioned Some Ukraine Efforts but Has Not Formalized Plans to Transition Others

NNSA has transitioned some of its nuclear and radiological security and safety efforts to its partners in Ukraine and has completed some emergency support efforts that it will not need to transition. NNSA intends to transition responsibility for some other nuclear and radiological security and safety efforts to Ukraine, and it is assessing Ukrainian partners' ability to independently sustain these efforts. However, the NNSA programs carrying out these efforts have not formalized their transition plans, including how they use their assessments of partner readiness in their planning.

NNSA Transitioned Certain Efforts to Ukrainian Partners

NNSA has transitioned some nuclear and radiological security and safety efforts to Ukrainian partners, according to NNSA officials. These officials described examples of efforts they successfully transitioned to Ukrainian partners.[51]

[50]*See* 48 C.F.R. § 44.201-1; Department of Energy, *Quality Assurance*, Order 414.1E (Washington, D.C.: Dec. 18, 2024).

[51]We did not assess NNSA's planning for transitioning these efforts.

- **Nuclear forensics evidence collection.** NNSA established a capability in Ukraine to collect forensic evidence in the event of a nuclear incident. NNSA trained Ukrainian responders on how to sustain this competency among their forensics collectors. This effort culminated in a "train-the-trainer" event at Idaho National Laboratory in August 2024. At that time, 17 regional teams and two national teams in Ukraine were equipped and trained to collect forensic evidence such as nuclear debris. According to NNSA, Ukraine is working to expand its corps of forensics collectors without direct U.S. assistance.
- **Nuclear and radiological emergency response training.** NNSA revised a training module to prepare local administrative authorities and community leaders in Ukraine to protect civilians during nuclear and radiological emergencies. The agency worked with local training staff in Ukraine to design the training materials. NNSA then held a train-the-trainer event in January 2025, during which it transferred the training materials to its Ukrainian partner. According to NNSA, the partner is now responsible for delivering the training and is incorporating the materials into its standard curricula.
- **Management of remote sensor data.** Through its remote sensing initiative, NNSA helped develop the capability to collect data in the event of a nuclear or radiological release in or around Ukraine.[52] As part of this initiative, NNSA provided two gamma spectrometers and a high-volume particulate air sampler to the State Space Agency of Ukraine to improve its ability to monitor and characterize nuclear and radiological incidents.[53] DOE and NNSA provided follow-up training to Ukrainian partners on how to independently use and maintain this equipment. NNSA officials told us they anticipate that after a year, Ukraine will assume full responsibility for all aspects of operating the air sampler, which was expected to enter operation by March 12, 2025. NNSA has completed transition of data management for dose rate sensors provided to Ukrainian partners. As part of this transition, in November 2024, NNSA provided initial training to 12 Ukrainian partners, which included trainers of additional users. NNSA officials told us they also provided Ukraine with 30 3-year user licenses and handed over the fully operational capability to Ukrainian partners.

Some NNSA programs that provided short-term support in response to temporary, emergency conditions in Ukraine have completed those efforts so they will not need to transition them. According to NNSA officials, certain efforts did not require prolonged sustainment, such as supplying chemicals and fuel for nuclear power plants to ensure their safe operation.

NNSA Intends to Transition Other Efforts to Ukrainian Partners

NNSA intends to transition other programmatic lines of effort to Ukrainian partners. NNSA offices provided us with estimated time frames for the lines of effort that they intend to transition to Ukrainian partners or the conditions they believe necessary for successful transition of responsibility (see table 5).

[52]The mission of the remote sensing initiative is to establish and sustain remote data acquisition to enable lab subject matter experts to make assessments that can inform decision-makers and public health officials. The transition of data management preserved the capability for Ukrainian partners to share data with U.S. stakeholders.

[53]The air sampler collects dust, smoke, and other aerosols on a large filter, which is then measured using the high-resolution gamma spectrometers. This combination of equipment provides very sensitive measurements that quantify small amounts of airborne radionuclides that can then be analyzed to discriminate among different types of nuclear incidents.

Table 5: Lines of Effort That the National Nuclear Security Administration (NNSA) Intends to Transition to Ukrainian Partners

NNSA program office	Line of effort	Estimated transition time frame
Nuclear Smuggling Detection and Deterrence	Install radiation portal monitors at border crossings and conduct training	2028
Office of Radiological Security	Protect sites that house radiological materials and provide secure transportation	When conflict ends or security situation stabilizes
Counterterrorism and Counterproliferation	Install sensors to remotely detect radiation release, and provide maintenance for these sensors	When conflict ends or security situation stabilizes

Source: GAO analysis of NNSA documents. | GAO-25-108444

NNSA officials for these programs provided details on how they intend to transition these efforts, which are omitted because the information is sensitive.

NNSA Programs Assess Partner Capabilities to Independently Sustain Efforts but Have Not Formalized Transition Plans Informed by These Assessments

NNSA programs assess Ukrainian partners' ability to independently sustain the nuclear and radiological security and safety efforts in accordance with leading practices for program management. However, NNSA programs have not formalized transition plans that document activities needed to achieve benefits or how assessments of partner capability will be used to inform transition planning. Assessing the receiving organization's readiness is a leading practice from the Project Management Institute's *The Standard for Program Management* for transitioning efforts before winding down a program.[54] NNSA's programs conduct their assessments of Ukrainian partners' capabilities using a range of metrics.[55]

Nuclear Smuggling Detection and Deterrence. NSDD has developed a Counter Nuclear Smuggling Assessment metric and associated indicators. NSDD uses this metric to conduct a quarterly assessment of partner capacity to prevent smuggling. The NSDD country team assessed data against this metric using five yes/no questions. See table 6 for a description of this metric.

Table 6: The Nuclear Smuggling Detection and Deterrence Program's Counter Nuclear Smuggling Assessment Metric

Category of indicators	Description
Policies and procedures	Does the partner agency have a formal, documented concept of operations defining its roles and responsibilities for operating counter nuclear smuggling measures?
Nuclear Security Detection Architecture operations	Does the partner agency consistently operate its counter nuclear smuggling measures in accordance with the concept of operations?

[54]The Project Management Institute is a not-for-profit organization that has established standards for program and project management that are generally recognized as leading practices for most programs and projects. These standards are used worldwide and provide guidance on how to manage various aspects of projects, programs, and portfolios. Project Management Institute, Inc., *The Standard for Program Management,* Fifth Edition (2024).

[55]In this report, we use "metric" to describe indicators, and sets of indicators organized into categories, for assessing partner capabilities.

Category of indicators	Description
Training	Are the partner agency's relevant personnel trained on the required knowledge and skills to conduct its counter nuclear smuggling measures?
Maintenance	Is the partner agency's radiation detection equipment maintained, operational, and capable of fulfilling the counter nuclear smuggling mission?
Assessment	Is the effectiveness of the partner agency's counter nuclear smuggling system routinely evaluated?

Source: GAO analysis of National Nuclear Security Administration information. | GAO-25-108444

NSDD provided information about its assessments against this metric, which is omitted because it is sensitive.

Office of Radiological Security. ORS has established country-level and site-level indicators to assess partners' readiness to manage and maintain physical security systems, which are summarized in table 7. ORS provided additional information about using these indicators, which was omitted because it is sensitive.

Table 7: Examples of Office of Radiological Security (ORS) Country- and Site-Level Indicators

Level	Category of indicator	Examples[a]
Country	Regulatory development	Does the country have regulations surrounding radiological source security, inventorying, and registration?
Country	Security inspection planning	Do the country's inspection teams have the authority to enter sites, conduct unannounced visits, and enforce compliance?
Country	Transportation security	Does the country ship sources through licensed transportation agents, give advanced notice of planned shipments, and conduct security inspections of shippers and carriers?
Country	National response engagement	Does the country have a radiological theft response plan that identifies stakeholder roles, establishes a hierarchy, and defines communication channels?
Country	Comprehensive inventory	Does the country have a national source registry, search and secure procedures, and a source disposal process?
Site	Security plan development	Have site personnel identified someone responsible for security, have they established procedures to operate the physical protection system, and do they periodically review and update the security plan?
Site	Site/responder interaction	Do site personnel know key responder contacts, have site and response personnel received alarm response training, and does the site have an alarm response plan appropriate to its response capability?
Site	Training/job knowledge	Are site personnel trained in the use of ORS-provided equipment, cybersecurity, and the threats, risks, and consequences that underpin procedures?
Site	Maintenance/testing	Does the site have written procedures that direct periodic preventative maintenance, maintain records of warranty and testing, and track maintenance problems and their corrective actions?
Site	Budget/life cycle planning	Does the site have someone responsible for budget planning, does management understand types of costs associated with security components, and is the site paying for costs previously covered by ORS?

Source: GAO analysis of National Nuclear Security Administration information. | GAO-25-108444

[a]ORS uses 47 national-level and 38 site-level yes/no questions for its assessments. This table includes examples from each category.

Other DNN offices, such as the Office of International Nuclear Security, have provided short-term support in response to temporary, emergency conditions that do not require prolonged sustainment planning, such as

supplying emergency backup diesel generators to nuclear power plants.[56] The Office of Nonproliferation and Arms Control will continue its support for IAEA.

CTCP officials told us that the office plans to continue certain efforts, but the details of those efforts are sensitive and have been omitted.

Although the DNN and CTCP programs have assessed Ukrainian partners' capability, the programs have not formalized transition plans that document activities needed to transition responsibility for these efforts to Ukrainian partners, as called for in leading practices for program management. For example, the programs have not documented how they intend to use their assessments of partner capability to inform their plans.

NNSA officials told us that they encountered obstacles in planning to transition certain emergency preparedness efforts to Ukrainian partners. These obstacles included uncertainty about the duration of the conflict, the residual nuclear and radiological threat landscape, and Ukraine's ability to allocate resources to sustain certain capabilities. Additionally, officials told us that because Ukraine is under martial law, the partner agencies NNSA is working with during the conflict are different from those that would be responsible for these efforts in peacetime. CTCP officials said they have discussed transition planning with Ukrainian partners and carried out activities to build capacity related to nuclear incident preparedness, consequence management, and nuclear forensics capabilities, according to agency officials. However, these officials said the surrounding uncertainties prevent more definitive transition planning.

According to *The Standard for Program Management*, leading practices for program management include the following:

- Developing transition plans before winding down the program to help the receiving entity continue to achieve the effort's benefits. Specifically, the program should formally document the activities necessary to achieve the program's planned benefits, to ensure these benefits are realized over time.
- Ensuring the receiving entity has a clear understanding of what is required for that entity to successfully sustain these benefits.

By formalizing transition plans, including documenting how assessments of partner capability inform the transition, NNSA would ensure understanding within the agency and between NNSA and Ukrainian partner organizations on what is needed to successfully sustain U.S. investments in nuclear and radiological safety and security in Ukraine without further NNSA support.

[56]The Office of International Nuclear Security also supported repairs and upgrades—such as to mitigate potential sabotage—at nuclear power plants under Ukrainian control and additional cybersecurity training and equipment to plant operators.

Conclusions

Russia's 2022 invasion of Ukraine has elevated nuclear and radiological security and safety dangers in the region. NNSA has responded through a range of important programmatic efforts supported by supplemental funding to prevent, prepare for, and mitigate the consequences of a nuclear or radiological incident. Some of these efforts were an extension of prior NNSA programs, and some involved new activities. NNSA relied on contractors to implement these efforts, and NNSA executed supplemental funding quickly and sometimes under conditions that limited direct oversight.

While NNSA and some contractors identified controls they implemented to manage fraud risks, NNSA did not conduct a fraud risk assessment tailored to the operating environment prior to the design of the controls and the execution of the funds. As a result, it is not clear that the controls NNSA and contractors used to manage fraud were risk-informed and appropriate. By updating its fraud risk guidance to specify the circumstances under which NNSA and other DOE programs should undertake fraud risk assessments—such as a change in the services a program is providing or the conditions under which it is operating—DOE could ensure a more consistent and timely approach to fraud risk management by programs that may need to execute activities and expend funds quickly, may have constrained oversight, or operate under other new or challenging circumstances.

NNSA has transitioned some nuclear and radiological security and safety efforts to Ukrainian partner organizations and intends to transition responsibility for some other efforts. However, NNSA programs have not formalized transition plans that document activities needed to sustain benefits or how they will use their assessments of partner capability to inform transition planning. NNSA faces uncertainties associated with the conflict in Ukraine that may limit its ability to plan to transition certain efforts. Documenting transition plans could help clarify, internally within NNSA and externally to Ukrainian partners, the operating conditions that NNSA considers necessary to successfully transition efforts. Formalizing such transition plans would also convey clear expectations to Ukrainian partner organizations, such as about the remaining work needed to prepare them to independently sustain nuclear and radiological security and safety efforts and the ways NNSA assesses those capabilities.

Recommendations

We are making two recommendations, including one each to DOE and NNSA:

The Office of Chief Financial Officer should update the Department of Energy's ERM guidance to require offices to conduct fraud risk assessments for programs that experience a structural change or a changed operating environment or that add new services, consistent with GAO's Fraud Risk Framework, and clarify the circumstances that could constitute a changed operating environment or addition of new services that should trigger a program-level assessment. (Recommendation 1)

The NNSA Administrator should ensure that the NNSA programs that have not yet done so formalize their plans for transitioning responsibility to Ukrainian partner organizations for future sustainment of NNSA-provided nuclear and radiological security and safety assistance, acknowledging that transition timing may be uncertain. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of the sensitive report to the Secretaries of Energy, State, and Defense, and to the Chairman of the NRC for review and comment. We received written comments on the sensitive report from DOE, reproduced in appendix III and summarized below.

In its comments, DOE agreed with our recommendations. Regarding the first recommendation, DOE said its Office of Chief Financial Officer would update DOE's ERM guidance for fiscal year 2026 to highlight that DOE offices should perform fraud risk assessments when they determine there are significant changes to their programs or operating environments. However, we specified that DOE's update should also include the addition of new program services as a circumstance that calls for a fraud risk assessment. Including this would fully address our recommendation. Regarding the second recommendation, DOE also said NNSA would formalize plans for transitioning efforts to Ukrainian partner organizations, as appropriate, by September 30, 2025.

DOE also provided technical comments on the sensitive report, which we incorporated as appropriate. NRC provided written comments on the sensitive report, which are reproduced in appendix IV, in which it indicated the agency had no comments. NRC officials provided an update in May 2025 in response to a draft of this public report, noting that in February 2025 NRC obligated the remaining $213,000 of the $2 million it received in supplemental appropriations, for regulatory training. State and DOD did not have any comments.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Energy, the Secretary of State, Secretary of Defense, Chairman of the NRC, and other interested parties. In addition, the report is 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 Allison Bawden at bawdena@gao.gov, or Nagla'a El-Hodiri at elhodirin@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 are listed in appendix V.

//SIGNED//

Allison Bawden
Director, Natural Resources and Environment

//SIGNED//

Nagla'a El-Hodiri
Director, International Affairs and Trade

List of Committees

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

The Honorable Lindsey Graham
Chairman
The Honorable Jeff Merkley
Ranking Member
Committee on the Budget
United States Senate

The Honorable James Risch
Chairman
The Honorable Jeanne Shaheen
Ranking Member
Committee on Foreign Relations
United States Senate

The Honorable Rand Paul, M.D.
Chairman
The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Mitch McConnell
Chair
The Honorable Christopher Coons
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Lindsey Graham
Chairman
The Honorable Brian Schatz
Ranking Member
Subcommittee on State, Foreign Operations, and Related Programs
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 Jodey Arrington
Chairman
The Honorable Brendan Boyle
Ranking Member
Committee on the Budget
House of Representatives

The Honorable Brian Mast
Chairman
The Honorable Gregory Meeks
Ranking Member
Committee on Foreign Affairs
House of Representatives

The Honorable James Comer
Chairman
The Honorable Stephen F. Lynch
Acting Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Ken Calvert
Chairman
The Honorable Betty McCollum
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

The Honorable Mario Diaz-Balart
Chairman
The Honorable Lois Frankel

Ranking Member
Subcommittee on National Security, Department of State, and Related Programs
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Division M of the Consolidated Appropriations Act, 2023, includes a provision for us to conduct oversight of the assistance provided in the Ukraine supplemental appropriations acts. Our report is part of a series of reports evaluating U.S. agencies' implementation of these funds in response to the crisis in Ukraine. This report (1) describes efforts the Department of Energy's (DOE) National Nuclear Security Administration (NNSA) and other key agencies have undertaken, or plan to undertake, to support nuclear and radiological security and safety for Ukraine; (2) examines the extent to which NNSA has taken steps to mitigate fraud risks in the nuclear and radiological security and safety efforts for Ukraine that were funded through supplemental appropriations; and (3) examines the extent to which NNSA has planned to transition certain nuclear and radiological security and safety efforts that were funded through supplemental appropriations to Ukrainian partners and ensure the sustainment of these efforts.

This report is a public version of a Controlled Unclassified Information (CUI) report that we issued in April 2025.[1] The National Nuclear Security Administration deemed some of the information in our April 2025 report to include CUI, which must be protected from public disclosure. Therefore, this report omits some information about certain program activities. Although the information provided in this report is more limited, the report addresses the same objectives as the CUI report and uses the same methodology.

To identify key agencies supporting nuclear and radiological security and safety in Ukraine, we first reviewed legislation, budgetary, and interagency and agency documentation. We also reviewed prior GAO reports, and interviewed agency officials for additional information. We identified the Department of State, Department of Defense (DOD), and Nuclear Regulatory Commission (NRC), in addition to NNSA, as key federal agencies.[2] We also included the International Atomic Energy Agency (IAEA), an autonomous international organization funded by member states, including the U.S., to which some of the Ukraine supplemental funding appropriated to NNSA was obligated.

To describe efforts NNSA, State, DOD, and NRC have undertaken to support nuclear and radiological security and safety in Ukraine, we reviewed agency budget documents, planning documents, and annual reports and interviewed officials from these agencies. We also reviewed IAEA documents and interviewed IAEA officials.

We assessed the reliability of U.S. agencies' data. To assess the reliability of DOE funding data, we reviewed and summarized information we previously collected about the Standard Accounting and Reporting System (STARS) and submitted follow-up questions to DOE to confirm this information was still accurate. These follow-up questions were about the specific data we are reporting, and how STARS generates financial data. We also submitted questions to State, DOD, and NRC asking how data were collected, processed, and reviewed.

[1]GAO, *Ukraine: DOE Could Better Assess Fraud Risks and Formalize Its Transition Plans for Nuclear Security and Safety Efforts*, GAO-25-107015SU (Washington, D.C.: Apr. 16, 2025). We also issued a separate classified annex to the CUI report that provides additional details on the nuclear and radiological security and safety risk environment in Ukraine and about certain actions NNSA is taking in response: GAO, *Classified Annex for GAO-25-107015SU: Additional Details on Nuclear and Radiological Security and Safety Risks in Ukraine*, GAO-25-107768C (Washington, D.C.: Apr. 16, 2025).

[2]We excluded other agencies with smaller roles, such as the Department of Health and Human Services, Department of Homeland Security, and Environmental Protection Agency.

Based on the information we obtained, we determined that the data were sufficiently reliable for the purposes of describing federal agency obligations in support of nuclear and radiological security and safety in Ukraine.

We identified nuclear and radiological security and safety risks driving these agencies' efforts by (1) reviewing intelligence assessments produced by DOE and written responses from Ukrainian agencies that we were able to obtain by working through State; and (2) interviewing NNSA and DOE officials. We interviewed Ukrainian officials to understand how they prioritize requests for U.S. support.

To examine the extent to which NNSA has taken steps to mitigate fraud risks in its efforts funded through the supplemental appropriations, we reviewed agency documents and interviewed agency officials and contractors.[3] Specifically, we reviewed DOE and NNSA guidance for mitigating fraud risk, interviewed NNSA and contractors who oversaw Ukraine-related efforts, and reviewed documentation of their contract oversight procedures. To further examine the extent to which NNSA took steps to mitigate fraud risks in its nuclear and radiological security and safety efforts for Ukraine, we collected information on the contract oversight and fraud risk mitigation approaches NNSA and contractors took on individual contracts by reviewing a nongeneralizable sample of contracts using Ukraine-related supplemental funding. In selecting this sample, we prioritized the contractors who received the largest amount of funding and used subcontractors to execute their work.

To do so, we reviewed DOE data on Ukraine supplemental funds overseen by contractors responsible for this work. We included in our sample all contractors that (1) received at least $1 million in funds and (2) those that issued subcontracts. We consulted DOE to verify that we had identified the contractors that fit these characteristics, resulting in a sample size of eight contractors and eight contracts. We conducted interviews with officials responsible for oversight of each of the eight contracts and requested documentation verifying the fraud mitigation and subcontract oversight processes described by these contractors in our interviews. Such documentation included cost-tracking spreadsheets, invoices, and photographs of delivered equipment and identifying characteristics, such as serial numbers. We also interviewed NNSA officials to understand how it works with contractors in the oversight process. Findings from our sample of eight selected contracts cannot be generalized to those we did not select and review.

Additionally, we reviewed DOE's Enterprise Risk Management (ERM) Fiscal Year 2024 Guidance, which contains fraud mitigation and internal controls policies, to understand the agency's approach to fraud risk management. We also interviewed DOE officials responsible for the department's ERM process and NNSA officials responsible for ensuring the agency follows ERM guidance. We compared DOE's ERM guidance with the leading practices identified in GAO's *A Framework for Managing Fraud Risk in Federal Programs*,[4] which contains leading practices that managers are directed to implement by the Office of Management and Budget.[5]

To examine the extent to which NNSA has planned to transition certain nuclear and radiological security and safety efforts to Ukrainian partners and ensure the sustainment of those efforts, we selected efforts supported

[3]We focused this objective on NNSA because, of the key agencies we examined, it received the most supplemental funding for nuclear and radiological security and safety in response to the invasion of Ukraine.

[4]GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 2015).

[5]Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control*, OMB Circular No. A-123 (July 15, 2016).

by supplemental appropriations.[6] To identify NNSA activities that would require sustainment planning, two analysts independently reviewed a list of NNSA-supported efforts to determine which were long-term in nature. We excluded assistance that was short-term or limited in scope, such as supplying chemicals and fuel for nuclear power plants to ensure their safe operation. In instances where the analysts had differing opinions, they discussed and found a resolution. We then asked NNSA which projects it planned to transition to its Ukrainian partners and requested information on its transition plans.

In response to our request, we reviewed information provided by NNSA programs outlining their intended approaches for transitioning future responsibility for certain efforts to Ukrainian partners, including information on goals and metrics the programs are using to assess Ukrainian partner capacity. We interviewed NNSA officials on their transition planning. We compared NNSA's plans against leading practices for program management and transition planning identified in the Project Management Institute's *The Standard for Program Management*.[7]

The performance audit upon which this report is based was conducted from September 2023 to April 2025 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. We subsequently worked with DOE from April 2025 through May 2025 to prepare this public version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

[6]We selected NNSA for our focus because, of the key agencies we examined, it received the most supplemental funding for nuclear and radiological security and safety in response to the invasion of Ukraine.

[7]Project Management Institute, Inc., *The Standard for Program Management*, Fifth Edition (2024).

Appendix II: National Nuclear Security Administration (NNSA) Contractors' Subcontract Oversight Procedures

To examine steps NNSA took to mitigate fraud risk in its nuclear security- and safety-related efforts for Ukraine funded by supplemental appropriations, we reviewed a nongeneralizable sample of NNSA's contracts supporting these efforts. We selected NNSA's eight largest contracts that involved subcontracted work; examined documentation associated with each, such as subcontractor payment records; and interviewed NNSA contracting officers and contractor representatives to understand how they mitigate fraud risk for their individual contracts and subcontracts. Six out of the eight contracts were management and operating (M&O) contracts to manage and operate Department of Energy (DOE) national laboratories and nuclear weapons production facilities.

Table 8: Examples of Subcontract Oversight and Fraud Mitigation Measures Identified by National Nuclear Security Administration (NNSA) and Its Prime Contractors for Nuclear Security and Safety Efforts for Ukraine Funded by Ukraine Supplemental Appropriations Acts

Prime contractor (site)	Subcontract scope of work	Subcontract type	Subcontract oversight processes
Battelle Memorial Institute (Pacific Northwest National Laboratory)	Monitoring radiological site security	Fixed price	Pre-award vetting through a technical and commercial evaluation of proposal and bidders
			Notified site office before awarding new or modifying existing subcontracts
Lawrence Livermore National Security, LLC (Lawrence Livermore National Laboratory)	High-performance computing	Fixed price	NNSA consent review[a]
Apogee Group, LLC	Supplying radiation monitoring equipment	Cost-plus-fixed-fee	NNSA required Apogee to obtain proof for every purchase
			NNSA monthly cost performance report to track cost variance
Honeywell Federal Manufacturing & Technologies, LLC (Kansas City National Security Campus)[b]	High-performance computing	Fixed price	Subcontract clause for screening counterfeit items
Mission Support and Test Services, LLC (Nevada National Security Site)	Capacity building, logistical support, and translations	Time and materials	Pre-award screening for subcontract risks, such as subcontractor financial health
			Subcontract clauses for screening counterfeit items
National Technology and Engineering Solutions of Sandia, LLC (Sandia National Laboratories)	Equipment delivery and training	Fixed price	Pre-award screening for subcontract risks, such as subcontractor financial health
University of Chicago Argonne, LLC (Argonne National Laboratory)	Delivery of emergency generators for nuclear power plants	Fixed price	Pre-award assessment of cost reasonableness
			Visited subcontractor facilities to verify capabilities

Prime contractor (site)	Subcontract scope of work	Subcontract type	Subcontract oversight processes
			Used photos and certificates of assembly to verify equipment installed
Project Enhancement Corporation	Counterterrorism and support for Nuclear Emergency Support Team	Time and materials	Monthly review of subcontractor deliverables before reimbursement
			Requires NNSA authorization for additional contracting hours

Source: GAO analysis of NNSA and contractor documents and interviews. | GAO-25-108444

[a]Under the Federal Acquisition Regulation, agencies should consider whether a proposed subcontract is appropriate to the risks involved and consistent with current policy when conducting a consent review. 48 C.F.R. § 44.202-2(a)(9). The Department of Energy (DOE) monitors contractors' compliance with subcontracting requirements by providing consent to the contractor to award certain subcontracts. DOE determines the subcontracts that require consent prior to award based on criteria the agency develops for each prime contract, such as subcontract dollar value and type of contract.

[b]Although the Kansas City National Security Campus contractor made this purchase, the Los Alamos National Laboratory received the computing equipment.

Appendix III: Comments from the Department of Energy

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

March 31, 2025

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 *Ukraine: DOE Could Better Assess Fraud Risks and Formalize Its Transition Plans for Nuclear Security and Safety Efforts* (GAO-25-107015SU). The Department of Energy's (DOE) National Nuclear Security Administration (NNSA) appreciates GAO's recognition of the planning and transition of activities to Ukraine that have been conducted to date.

NNSA agrees with GAO's recommendation to formalize plans for transitioning selected projects to Ukrainian partner organizations as appropriate, consistent with the current operating environment, as noted in the enclosed Management Decision. NNSA appreciates GAO's recognition that NNSA's risk assessment and controls in place at the contract level for the Ukraine projects are appropriate to the circumstances of operations and current guidance. NNSA notes that DOE's Office of the Chief Financial Officer agrees with GAO's recommendation to update the Enterprise Risk Management guidance to incorporate additional leading practices.

DOE/NNSA 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 George Webb, Acting Director, Audits and Internal Affairs, at (240) 306-7709.

Sincerely,

Teresa M. Robbins
Acting Under Secretary for Nuclear Security and Administrator, NNSA

Enclosure

NATIONAL NUCLEAR SECURITY ADMINISTRATION

Management Decision

Ukraine: DOE Could Better Assess Fraud Risks and Formalize Its Transition Plans for Nuclear Security and Safety Efforts (GAO-25-107015SU)

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

Recommendation 1: DOE's Office of the Chief Financial Officer (OCFO) update the Department's Enterprise Risk Management (ERM) guidance to require its offices to conduct fraud risk assessments for programs that experience a structural change, changed operating environment, or add new services, consistent with GAO's Fraud Risk Framework, and clarify the circumstances that could constitute a changed operating environment or addition of new services that should trigger a program-level assessment.

Management Response: Concur. The Department's ERM guidance currently requires DOE reporting organizations to adhere to the leading practices identified in the GAO Fraud Risk Framework, in alignment with 0MB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control.* Additionally, the Department's ERM guidance states that DOE reporting organizations may prepare risk profiles as their office deems appropriate. However, OCFO will update the Department's annual ERM guidance in fiscal year (FY) 2026 to clearly highlight that fraud risk assessments should be performed when DOE reporting organizations determine there are significant changes to their programs or operating environments. Additionally, OCFO is currently in the process of automating the Department's risk assessment and risk profile process to allow DOE reporting organizations to identify and assess significant fraud risks more effectively. This automated capability, which is expected to be rolled out in FY 2026 to DOE reporting organizations, will support more timely reporting of assessed fraud risks across the Department. The estimated date for completing these actions is March 31, 2026.

Recommendation 2: NNSA ensure that all applicable NNSA programs formalize their plans for transitioning responsibility to Ukrainian partner organizations for future sustainment of NNSA-provided nuclear and radiological security and safety assistance, acknowledging that transition timing may be uncertain.

Management Response: Concur. NNSA will formalize plans for transitioning efforts to Ukrainian partner organizations, as appropriate, while also considering the operational realities of the situation in Ukraine. The estimated date for completing this action is September 30, 2025.

Appendix IV: Comments from the Nuclear Regulatory Commission

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

March 11, 2025

Allison Bawden, Director
Natural Resources and Environment Team
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20226

Dear Director Bawden:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am responding to the U.S. Government Accountability Office (GAO) Draft Audit Report: "Ukraine: DOE Could Better Assess Fraud Risks and Document Transition Plans for Its Nuclear Security and Safety Efforts," (GAO-24-10701SSU), dated March 2025.

The NRC appreciates the opportunity to review the report. The NRC focused our review on sections applicable to us and finds that the GAO report accurately captures the NRC's actions. Further, we note that the report did not identify recommendations for the NRC. We do not have additional comments.

If you have any questions or need additional information, please contact me or have your staff contact John Jolicoeur by email at John.Jolicoeur@nrc.gov.

Sincerely,

Mirela Gavrilas
Executive Director for Operations

March 11, 2025

Nagla'a El-Hodiri, Director
International Affairs and Trade
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20226

Dear Director El-Hodiri:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am responding to the U.S. Government Accountability Office (GAO) Draft Audit Report: "Ukraine: DOE Could Better Assess Fraud Risks and Document Transition Plans for Its Nuclear Security and Safety Efforts," (GAO-24-107015SU), dated March 2025.

The NRC appreciates the opportunity to review the report. The NRC focused our review on sections applicable to us and finds that the GAO report accurately captures the NRC's actions. Further, we note that the report did not identify recommendations for the NRC. We do not have additional comments.

If you have any questions or need additional information, please contact me or have your staff contact John Jolicoeur by email at John.Jolicoeur@nrc.gov.

Sincerely,

Mirela Gavrilas
Executive Director for Operations

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Allison Bawden, bawdena@gao.gov

Nagla'a El-Hodiri, elhodirin@gao.gov

Staff Acknowledgments

In addition to the contacts named above, William Hoehn (Assistant Director), Jeremy Latimer (Assistant Director), Alisa Beyninson (Analyst in Charge), Irina Carnevale, Tara Congdon, and Eli Dile made key contributions to this report. Other staff who made contributions to the report include Adrian Apodaca, William Bauder, Antoinette Capaccio, Cindy Gilbert, Shannon Murphy, and Rebecca Shea.

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 X, LinkedIn, Instagram, and YouTube.
Subscribe to our 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

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us