United States Government Accountability Office

Report to the Committee on Armed Services, House of Representatives

May 2023

NUCLEAR SECURITY

DOE Should Take Actions to Fully Implement Insider Threat Program

GAO-23-105576

GAO Highlights

Highlights of GAO-23-105576 a report to the Committee on Armed Services, House of Representatives

May 2023

NUCLEAR SECURITY

DOE Should Take Actions to Fully Implement Insider Threat Program

Why GAO Did This Study

The theft of nuclear material and the compromise of information could have devastating consequences. Threats can come from external adversaries or from "insiders," including employees or visitors with trusted access. In 2014, DOE established its Insider Threat Program to integrate its policies, procedures, and resources. The program also coordinates analysis, response, and mitigation actions among DOE organizations.

The House report accompanying a bill for the National Defense Authorization Act for fiscal year 2022 includes a provision for GAO to review DOE's efforts to address insider threats with respect to the nuclear security enterprise. This report examines (1) the extent to which DOE has implemented required standards to protect the nuclear security enterprise from insider threats and (2) the factors that have affected DOE's ability to fully implement its Insider Threat Program.

GAO reviewed the minimum standards and best practices for federal insider threat programs, DOE documentation, and four assessments by independent reviewers. GAO also interviewed DOE and National Nuclear Security Administration officials and contractors.

What GAO Recommends

GAO is making seven recommendations to DOE, including (1) to track and report on actions it takes to address reviewers' findings and recommendations, (2) to establish a process to better integrate program responsibilities, and (3) to assess resource needs for the program. DOE agreed with the recommendations and described plans to address them.

View GAO-23-105576. For more information, contact Allison Bawden at (202) 512-3841 or BawdenA@gao.gov.

What GAO Found

The Department of Energy (DOE) has not implemented all required measures for its Insider Threat Program more than 8 years after DOE established it in 2014, according to multiple independent assessments. Specifically, DOE has not implemented seven required measures for its Insider Threat Program, even after independent reviewers made nearly 50 findings and recommendations to help DOE fully implement its program (see fig. for examples). DOE does not formally track or report on its actions to implement them. Without tracking and reporting on its actions to address independent reviewers' findings and recommendations, DOE cannot ensure that it has fully addressed identified program deficiencies.

Examples of Selected Recommendations from Independent Assessments of DOE's Insider Threat Program

Sources: GAO analysis of documents from Carnegie Mellon University, Department of Energy (DOE), the Office of the Director of National Intelligence, and National Aeronautics and Space Administration. | GAO-23-105576

DOE has not fully implemented its Insider Threat Program due to multiple factors.

- **DOE has not integrated program responsibilities.** DOE has not effectively integrated Insider Threat Program responsibilities. Instead, DOE divided significant responsibilities for its program between two offices. Specifically, the program's senior official resides within the security office, while operational control for insider threat incident analysis and response resides within the Office of Counterintelligence—a part of the organization with its own line of reporting to the Secretary of Energy. Without better integrating insider threat responsibilities between these offices, DOE's insider threat program will continue to face significant challenges that preclude it from having an effective or fully operational program.
- **DOE has not identified and assessed resource needs.** DOE has not identified and assessed the human, financial, and technical resources needed to fully implement its Insider Threat Program. Program funding identified in DOE's budget does not account for all program responsibilities. For example, DOE's budget does not include dedicated funding for its contractor-run nuclear weapons production and research sites to carry out their responsibilities for implementing the program. Unless DOE identifies and assesses the resources needed to support the Insider Threat Program, it will be unable to fully ensure that components are equipped to respond to insider threat concerns, potentially creating vulnerabilities in the program.

Contents

Abbreviations

DOE	U.S. Department of Energy
NASA	National Aeronautics and Space Administration
NDAA	National Defense Authorization Act
NNSA	National Nuclear Security Administration

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 24, 2023

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

The Department of Energy (DOE) has recognized that threats to its assets, such as special nuclear material and classified information, can come from "insiders," including employees or visitors with trusted access.[1] Such threats could have significant consequences for national security and could include unauthorized release of classified information; workplace violence; or improper access to sensitive nuclear weapons, material, and components. DOE has long-standing measures—including counterintelligence and physical and information security programs—to deter, detect, and respond to theft, diversion, destruction, or other misuse of its critical assets.

In 2011, in the wake of a high-profile unauthorized release of classified information involving an insider at a federal agency, the President issued Executive Order 13587 directing agencies to establish, implement, monitor, and report on the effectiveness of insider threat programs to protect national security information on computer networks.[2] This led DOE to issue Order 470.5 and establish an Insider Threat Program for the agency in 2014.[3] The DOE order expanded the initial focus of the executive order on classified information and systems to include threats to personnel, facilities, material (including special nuclear material), information, and equipment. DOE's program is in addition to, and did not replace, existing protective measures at agency facilities. According to the agency's order, its Insider Threat Program is intended to integrate insider threat-related policies, procedures, and resources across DOE,

[1]"Special nuclear material" includes plutonium and uranium enriched in the isotope 233 or in the isotope 235.

[2]Executive Order 13587, *Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information* (Oct. 7, 2011).

[3]U.S. Department of Energy, DOE Order 470.5, *Insider Threat Program* (June 2, 2014).

including at DOE sites.[4] The program is also intended to coordinate insider threat analysis, response, and mitigation actions among the relevant DOE component organizations, including DOE counterintelligence, security, legal counsel, inspector general, and human capital, and with law enforcement agencies.

The loss, theft, diversion, or misuse of DOE assets, such as special nuclear material and classified information, could have significant consequences for national security and public safety. The National Nuclear Security Administration (NNSA)—a separately organized agency within DOE—is responsible for maintaining the U.S. nuclear weapons stockpile and overseeing the sites for weapons production and research, collectively known as the nuclear security enterprise.[5] NNSA relies extensively on contractors with trusted access to carry out its missions through the management and operation of these facilities.

House Report 117-118, accompanying H.R. 4350, a bill for the National Defense Authorization Act (NDAA) for fiscal year 2022, includes a provision for GAO to review DOE's efforts to address insider threats with respect to the nuclear security enterprise. This report examines (1) the extent to which DOE has implemented required standards to protect the nuclear security enterprise from insider threats and (2) the factors that have affected DOE's ability to fully implement its Insider Threat Program.

The scope of our review focuses on DOE's implementation of its Insider Threat Program at the eight sites in the nuclear security enterprise.[6] For

[4]As of January 2023, DOE had 23 contractor-managed and -operated sites through the country.

[5]The nuclear security enterprise comprises a network of eight government-owned, contractor-operated research laboratories and nuclear weapons production facilities that provide the research, development, testing, and production capabilities needed to maintain and modernize our nation's nuclear weapons stockpile and related infrastructure. We refer to these laboratories and facilities as sites. These eight sites are the Kansas City National Security Campus in Missouri; the Lawrence Livermore National Laboratory in California; the Los Alamos National Laboratory in New Mexico; the Nevada National Security Site, formerly known as the Nevada Test Site, in Nevada and other locations; the Sandia National Laboratories in New Mexico and other locations; the Pantex Plant in Texas; the Y-12 National Security Complex in Tennessee; and NNSA operations at DOE's Savannah River Site in South Carolina.

[6]DOE's Insider Threat Program is department wide; however, for the purposes of this review, we reviewed DOE's implementation of the program at the eight sites in the nuclear security enterprise.

this review, we obtained documentary and testimonial evidence from DOE, management and operating contractors at sites in the nuclear security enterprise, and other organizations outside of DOE that have reviewed DOE's program. For example, we reviewed DOE program documentation, including the most recent annual report covering calendar year 2017, the most recent strategic plan for the Insider Threat Program covering fiscal years 2017 through 2020, and local program charters and management and operating contracts. We also interviewed officials from DOE's Office of Security and Office of Counterintelligence and officials from NNSA's Office of Defense Nuclear Security.

In addition, we conducted semistructured interviews with DOE officials and contractors responsible for implementing the Insider Threat Program at the eight sites in the nuclear security enterprise. Further, we reviewed independent assessments of DOE's Insider Threat Program conducted by Carnegie Mellon University's Insider Threat Center,[7] the National Aeronautics and Space Administration's (NASA) Independent Verification and Validation Program,[8] DOE's Office of Enterprise Assessments,[9] and the National Insider Threat Task Force.[10] We identified key findings or recommendations for DOE's Insider Threat Program made in these independent assessments and categorized them into nine topic areas in appendix II. In addition, to determine the current status of these findings and recommendations, we reviewed program performance documentation and interviewed DOE officials and officials responsible for producing these assessments.

To determine the extent to which DOE has implemented required measures to protect the nuclear security enterprise from insider threats, we reviewed requirements for federal insider threat programs, including

[7]Carnegie Mellon University, Software Engineering Institute, Computer Emergency and Response Team Insider Threat Center, *Insider Threat Program Evaluation: Department of Energy* (Mar. 2015).

[8]National Aeronautics and Space Administration Independent Verification and Validation Program, *Phase 1 Summary Report* (Washington, D.C.: Dec. 17, 2015).

[9]U.S. Department of Energy, Office of Safeguards and Security Assessments, Office of Enterprise Assessments, *Special Assessment of the Department of Energy's Insider Threat Program* (June 2021).

[10]Director of National Intelligence, *National Insider Threat Task Force Assessment of the Department of Energy's Insider Threat Program Pursuant to Executive Order 13587 and the National Insider Threat Policy and Minimum Standards* (Washington, D.C.: Mar. 8, 2022).

Executive Order 13587; the *National Insider Threat Policy* and *Minimum Standards for Executive Branch Insider Threat Programs* (minimum standards);[11] and DOE Order 470.5: *Insider Threat Program*. We also reviewed related guides for implementing those standards, such as the 2017 *Insider Threat Guide* and the *Insider Threat Program Maturity Framework* produced by the National Insider Threat Task Force,[12] and recommendations in GAO's Framework of Key Elements for the Department of Defense's Insider Threat Programs.[13] We compared requirements established in the minimum standards and DOE's order with information from our document reviews and interviews.

To determine the factors that have affected DOE's ability to implement an effective Insider Threat Program, we analyzed agency documentation, including the agency's 2014 *Insider Threat Program Implementation Plan* and its *2017-2020 Strategic Plan*. We interviewed DOE officials and management and operating contractors at sites in the nuclear security enterprise to identify the root causes that have affected DOE's ability to meet program requirements. We compared DOE's plans and actions with best practices for insider threat programs produced by the National Insider Threat Task Force.

We conducted this performance audit from December 2021 to May 2023, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

[11]National Insider Threat Task Force, *National Insider Threat Policy* and *Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 21, 2012).

[12]National Insider Threat Task Force, *Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards* (2017); and *Insider Threat Program Maturity Framework* (Nov. 1, 2018).

[13]GAO, *Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems*, GAO-15-544 (Washington, D.C.: June 2, 2015).

Insider Threat Measures at DOE

According to the *National Insider Threat Policy*, an insider is any person with authorized access to any government or contractor resource, to include personnel, facilities, information, equipment, networks, or systems.[14] An insider threat is the chance that an individual will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States, including through espionage, terrorism, unauthorized disclosure of classified information, or through the loss or degradation of government resources or capabilities.[15]

As of 2022, DOE had over 13,000 federal employees, and its management and operating contractors and other contractors employed over 120,000 people, who, because of their authorized access to DOE facilities and networks, can be considered to be insiders.[16] DOE has used multiple defensive measures to deter, detect, and respond to misuse of critical assets. These measures include, for example, programs that vet personnel for security and reliability. Specifically, employees and contractors requiring access to sensitive nuclear information and material must obtain special security clearances. Currently, according to DOE officials, a significant percentage of DOE employees and contractors have these clearances.[17]

According to DOE officials, many of these individuals across DOE—a majority of whom are contractors—are also subject to additional scrutiny

[14]The *National Insider Threat Policy* was issued by the National Insider Threat Task Force, which is under the joint leadership of the Attorney General and the Director of National Intelligence and is staffed by employees and contractors from a variety of agencies, including the Federal Bureau of Investigation, the National Counterintelligence and Security Center within the Office of the Director of National Intelligence, the Defense Intelligence Agency, the Central Intelligence Agency, and the Transportation Security Administration. According to a presidential memorandum transmitting the policy, it is to provide direction and guidance to promote the development of effective insider threat programs to deter, detect, and mitigate actions by employees who may represent a threat to national security.

[15]National Insider Threat Task Force, *National Insider Threat Policy* and *Minimum Standards for Executive Branch Insider Threat Programs.*

[16]Management and operating contracts are agreements 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 of the major programs of the contracting federal agency. 48 C.F.R. § 17.601.

[17]According to DOE officials, many federal employees at other agencies also hold clearances to access sensitive nuclear information.

through the Human Reliability Program, which is intended to ensure that only individuals who meet the highest standards of reliability and physical and mental suitability have access to certain materials, nuclear explosive devices, and facilities.[18] To protect DOE's networks and information, DOE's Office of the Chief Information Officer also leads a cybersecurity program that continuously monitors activity to detect and mitigate unauthorized intrusions.

In addition to programs that focus on personnel vetting, DOE and NNSA maintain layered physical security measures within nuclear weapons facilities to minimize the probability that cleared personnel can engage in improper conduct. For example, sites may use an array of sensors and inspections to monitor sensitive areas. DOE and NNSA also use a protocol, where authorized persons responsible for maintaining control of sensitive items, such as nuclear explosives, must be physically located where they have an unobstructed view of each other or the items. Other physical security measures include highly trained and armed on-site security forces to respond quickly to any security incident.

Requirements for Federal Agencies

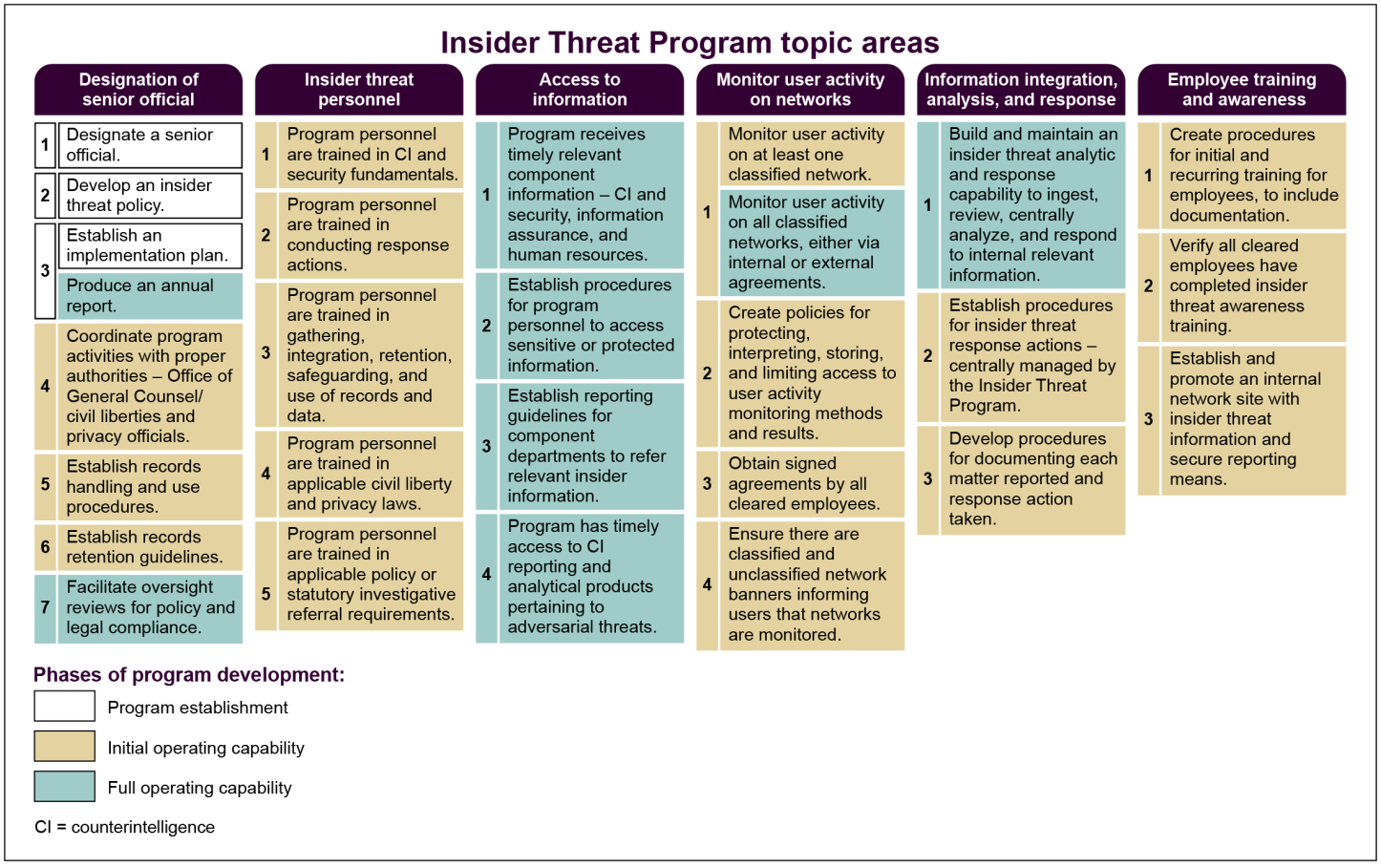
In 2011, additional requirements to deter, detect, and mitigate insider threats to classified information and systems were placed on all agencies, after a high-profile unauthorized disclosure of classified information by a U.S. Army intelligence analyst. Specifically, Executive Order 13587 directed agencies to designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts for the agency and to implement an insider threat detection and prevention program.

The executive order also created the National Insider Threat Task Force to produce a government-wide policy for the deterrence, detection, and mitigation of insider threats and minimum standards and guidance for agency implementation of this policy. Consequently, in 2012, the National Insider Threat Task Force issued the *National Insider Threat Policy* and *Minimum Standards for Executive Branch Insider Threat Programs*, which included 26 minimum standards, under six topic areas, which agencies'

[18]The objective of the Human Reliability Program is accomplished through a system of continuous evaluation that identifies individuals whose judgment and reliability may be impaired by physical or mental/personality disorders, alcohol abuse, use of illegal drugs, the abuse of legal drugs or other substances, or any other condition or circumstance that may be of a security or safety concern. 10 C.F.R. § 712.1.

programs should meet (see fig. 1).[19] According to the task force, these minimum standards provide the basic elements necessary for an agency to establish an effective Insider Threat Program. The task force defined three phases of program development based on the number and type of minimum standards that a program has implemented. These phases are (1) program establishment, (2) initial operating capability, and (3) full operating capability.

Figure 1: Summary of the 26 Minimum Standards for Executive Branch Insider Threat Programs

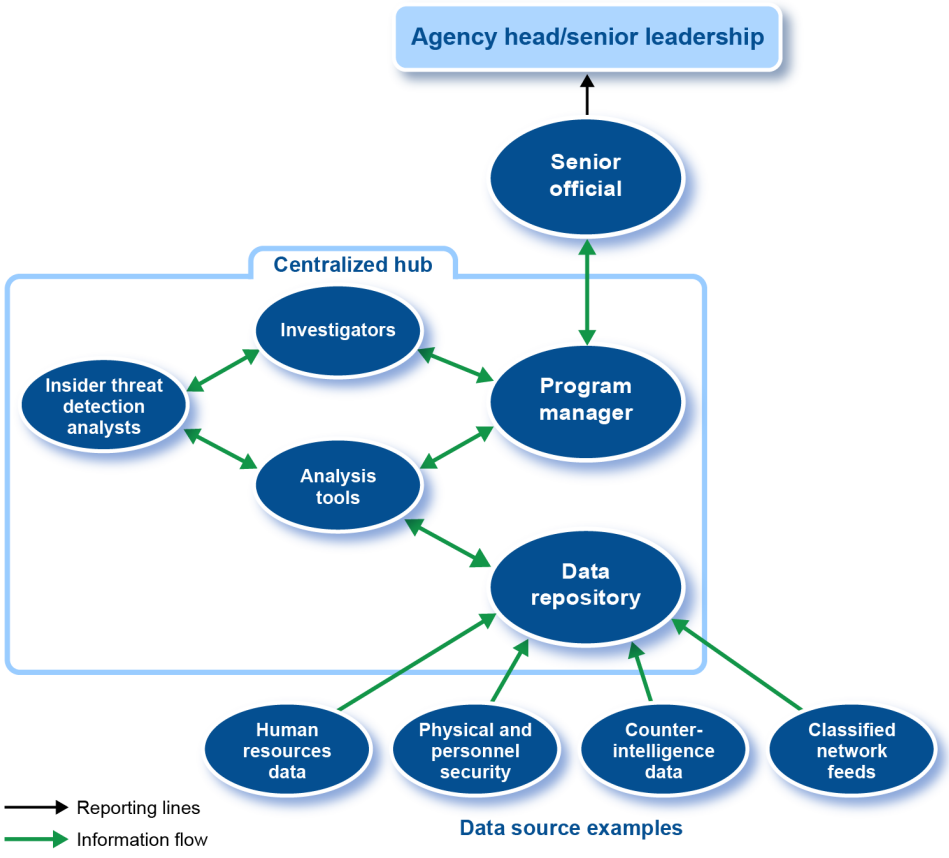


Source: Department of Justice, Office of the Director of National Intelligence. | GAO-23-105576

[19]National Insider Threat Task Force, *National Insider Threat Policy* and *Minimum Standards for Executive Branch Insider Threat Programs.*

The National Insider Threat Task Force also produced several guides for agencies to use when developing insider threat programs. These include the *Guide to Accompany the National Insider Threat Policy and Minimum Standards* in 2013, and the most recent guidance found in the 2017 *Insider Threat Guide* and the *Insider Threat Program Maturity Framework* that focus on continuous program improvement. Guidance from the National Insider Threat Task Force includes recommended practices for structuring an effective Insider Threat Program, such as using a centralized "hub" for insider threat analysis and response (see fig. 2).

Figure 2: Selected Elements of the National Insider Threat Task Force's Recommended Structure for an Insider Threat Program



Source: National Insider Threat Task Force *2017 Insider Threat Guide*. | GAO-23-105576

DOE's Insider Threat Program

To comply with the requirements established by Executive Order 13587, DOE issued Order 470.5 in 2014, which created an Insider Threat

Program for the entire agency, including for NNSA. Per this order, DOE's Insider Threat Program was intended to integrate the agency's various security, intelligence, and personnel programs into a comprehensive effort to deter, detect, and mitigate insider threats. In addition, the DOE order expanded on the executive order's initial focus—the unauthorized release of classified information—to include threats to personnel, facilities, material (including special nuclear material), information, and equipment. According to DOE's strategic plan for the program, DOE's Insider Threat Program does not introduce a new protective measure into the agency, but rather is intended to integrate preexisting measures into a comprehensive management framework for insider risk.[20] Figure 3 illustrates types of insider threats that DOE faces, including threats involving fraud, espionage, and terrorist activity.

Figure 3: The Types of Threats Covered by the Department of Energy's Insider Threat Program

Source: Department of Energy. | GAO-23-105576

[20]U.S. Department of Energy, *Department of Energy Insider Threat Program Strategic Goals and Objectives, 2017-2020*.

With DOE Order 470.5, DOE established several new functions with responsibilities for managing and carrying out its Insider Threat Program. These included the

- **designated senior official (senior official)**. This official is responsible for providing direction, guidance, and oversight of the program;
- **Insider Threat Analysis and Referral Center (Analysis and Referral Center)**. This center is intended to serve as the hub for insider threat information by centrally collecting, integrating, reviewing, assessing, and initiating referrals or appropriate responses based on information from intelligence, counterintelligence, security, information technology, information assurance, human resources, law enforcement, and other sources as necessary and appropriate;[21] and
- **Local Insider Threat Working Groups**. These groups are located at each of the eight sites in the nuclear security enterprise and other DOE sites. The groups are responsible for developing and maintaining a collaborative environment to identify, coordinate, and integrate local activities to address insider threats. They are to maintain awareness of all factors affecting the risk from insider threats, facilitate access to local data to support the Analysis and Referral Center, and coordinate activities to assist local authorities to ensure that local insider threat data and records are developed, maintained, shared, and protected, as required. These groups are comprised of both contractor and federal employees.

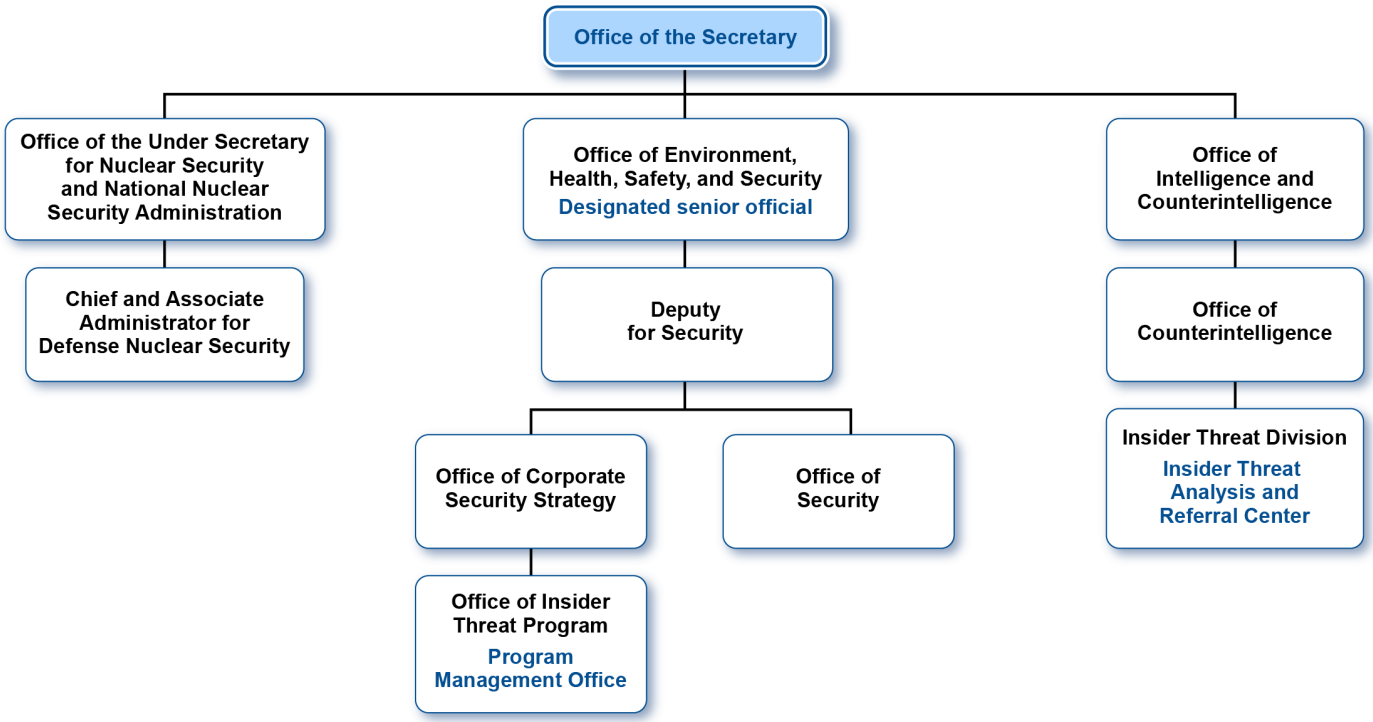
DOE Order 470.5 identifies a number of DOE components that have responsibilities for supporting the Insider Threat Program, including (1) the DOE General Counsel; (2) the Office of Intelligence and Counterintelligence; (3) the Office of Environment, Health, Safety, and Security; (4) the Office of the Chief Information Officer; (5) the Office of the Chief Human Capital Officer; (6) DOE program and staff offices; and (7) NNSA. In addition, DOE's Office of Enterprise Assessments performs independent assessments for DOE leadership that report on whether national security material and information assets are appropriately protected and whether departmental operations provide for the safety of its employees and the public.

[21]Per DOE Order 470.5, an insider threat response is an activity conducted to ascertain whether certain matters or information indicate the presence of an insider threat, as well as activities to mitigate the threat.

Among DOE components with Insider Threat Program responsibilities, two components share primary responsibility for the key functions described above, according to DOE officials (see fig. 4). These components are

- **The Office of Environment, Health, Safety, and Security**. The Secretary of Energy designated a senior official for the Insider Threat Program from within the Office of Environment, Health, Safety, and Security, and DOE created an Office of Insider Threat Program within the Office of Corporate Security Strategy—a suboffice within Environment, Health, Safety, and Security—to support the senior official and carry out specific program responsibilities; and
- **The Office of Intelligence and Counterintelligence**. DOE Order 470.5 identifies the Office of Intelligence and Counterintelligence as responsible for providing funding and facilities for the Analysis and Referral Center and for establishing the Local Insider Threat Working Groups at DOE sites.

Figure 4: Offices with Key Responsibilities for the Department of Energy's Insider Threat Program



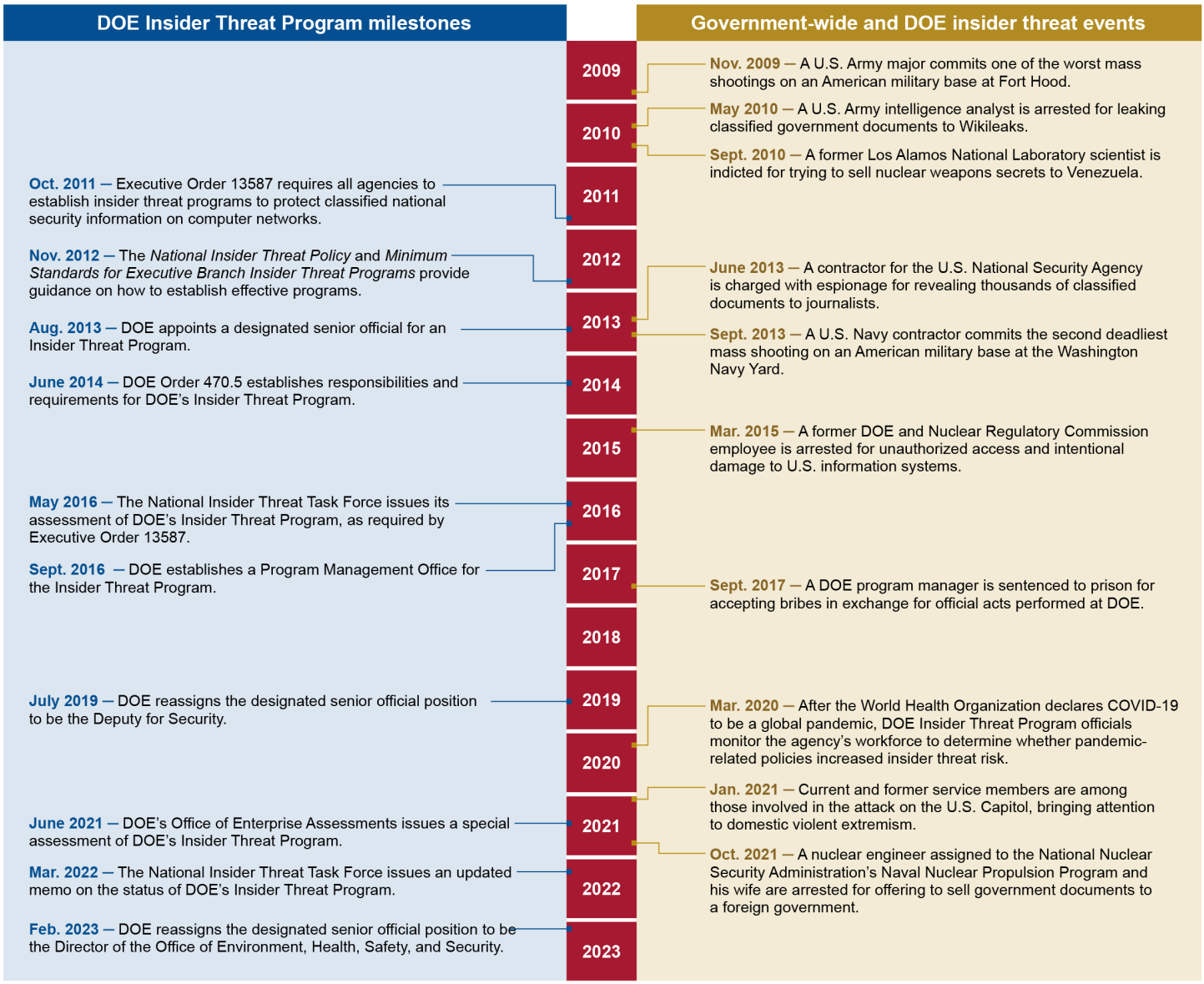
Source: GAO analysis of Department of Energy (DOE) documents. | GAO-23-105576

Note: In addition to the offices shown above, the following offices have responsibilities for DOE's Insider Threat Program per DOE Order 470.5: DOE General Counsel, Office of the Chief Information Officer, Office of the Chief Human Capital Officer, and DOE program and staff offices.

DOE reported experiencing about 250 unclassified insider threat-related security incidents in 2017, according to the annual report from its Insider Threat Program for that year—the most recent year for which DOE reported data. DOE considered about 100 of those incidents to be serious.[22] The report stated that most incidents were unintentional. Such incidents included sending classified information over unclassified systems, leaving security areas unattended, and not properly protecting classified information. However, the report identified several incidents considered to have been malicious. For example, the report described a highly publicized incident in which an individual was found guilty of accepting nearly $500,000 in bribes in exchange for official acts he performed in his capacity at the agency. That individual was subsequently sentenced to 18 months in prison and required to pay restitution. Figure 5 summarizes key events in DOE's efforts to establish its Insider Threat Program and examples of insider threat-related incidents at DOE and elsewhere in federal government.

[22]U.S. Department of Energy, *Insider Threat Program 2017 Annual Report* (June 19, 2018).

Figure 5: Key Events in the Establishment of DOE's Insider Threat Program and Recent Insider Threat Events Involving Federal Employees and Contractors



Sources: Department of Energy (DOE) documentation and GAO analysis. | GAO-23-105576

DOE Has Not Fully Implemented Requirements for Its Insider Threat Program or Addressed Long-Standing Recommendations

More than 8 years after DOE established its Insider Threat Program in 2014, DOE has not met all requirements for its program to be considered fully operational, according to multiple independent reviewers. Further, DOE has not made significant progress to address long-standing findings and to implement the recommendations from those reviewers.

Independent Assessments Found That DOE Has Not Fully Implemented Minimum Standards for Its Insider Threat Program

DOE has not fully implemented seven of the 26 minimum standards for its Insider Threat Program to reach full operating capability, according to our analysis of independent assessments conducted of the program. Executive Order 13587 directs the National Insider Threat Task Force to assess the adequacy of each federal agency's program to implement the established policies and minimum standards. The National Insider Threat Task Force completed its initial assessment of DOE's Insider Threat Program in 2016.[23] In addition, the *National Insider Threat Policy* directs federal agencies to conduct self-assessments of compliance with insider threat policies and standards. DOE officials told us that they requested assessments from three independent reviewers to assist with the establishment of its Insider Threat Program and to meet minimum standard requirements. Specifically, DOE requested assessments from NASA's Independent Verification and Validation Program (2015),[24]

[23]Office of the Director of National Intelligence entities, including the National Insider Threat Task Force and the National Counterintelligence and Security Center, conducted multiple assessments of DOE's Insider Threat Program from 2016 to 2020, which are classified. In addition, in March 2022, the Director of National Intelligence sent a follow-up memo to the Secretary of Energy, which summarizes the key findings and recommendations from previous assessments in an unclassified format.

[24]NASA received about $1.3 million to provide technical assistance to DOE's Insider Threat Program, according to NASA officials. NASA officials told us that they had a second agreement to provide ongoing technical assistance through 2025 for about $1.7 million, but they ended their review in October 2021 due to a lack of progress by DOE in implementing NASA's recommendations. Further, NASA substantially reduced the terms of its second agreement with DOE and ended the agreement early in May 2022, effectively bringing the technical assistance to an end.

Carnegie Mellon University's Insider Threat Center (2015), and DOE's Office of Enterprise Assessments (2021).[25]

Four of the seven unmet minimum standards were identified in a March 2022 memo that the Director of National Intelligence issued to the Secretary of Energy on behalf of the National Insider Threat Task Force as a follow-up to its 2016 assessment and recommendations. Information we received from DOE about the current status of the Insider Threat Program confirms that these four minimum standards remain unmet by the program:

- **Initial and recurring employee training**. Under the "employee awareness and training" topic area, the minimum standards require that federal agencies provide insider threat awareness training to all cleared employees within 30 days of initial employment, or following the granting of access to classified information, and annually thereafter.[26] According to the standards, training should address current and potential threats in the work and personal environment and should include topics such as indicators of insider threat behavior and incident reporting procedures. However, as of January 2023, DOE Order 470.5 does not require such training to be annual, and training implementation has been inconsistent across DOE sites, according to DOE officials. According to an internal memo from June 2022, DOE officials suggested that DOE Order 470.5 should be updated to include an annual training requirement, but DOE has not implemented the change.
- **Verification of insider threat awareness training**. Also under the "employee awareness and training" topic area, minimum standards require that federal agencies verify that all cleared employees have completed the required insider threat awareness training. In July 2020, DOE began using a new system to conduct and track completion of the required training for all cleared employees and contractors. However, in June 2021, DOE's Office of Enterprise Assessments found that DOE had not ensured that cleared employees received both the initial and annual training with required

[25]In addition to these independent reviewers, in March 2023, DOE's Office of Inspector General issued a more narrowly scoped assessment of DOE's Insider Threat Program, with a focus on the program's Insider Threat Analysis and Referral Center.

[26]DOE Order 470.5 extends the requirement for insider threat awareness training to all cleared DOE employees and contractors.

content.[27] Furthermore, as of August 2022, DOE could not fully validate training completion, according to DOE officials, because contractors are not required to use the new system, and many continue to use local systems to track training completion internally.

- **Oversight reviews for policy and legal compliance**. Under the "designation of senior official" topic area, minimum standards require that the senior official of an agency's Insider Threat Program facilitate oversight reviews to ensure compliance with insider threat policy guidelines, as well as applicable legal, privacy, and civil liberty protections. DOE previously contracted with some of the independent reviewers described above to receive assessments of its Insider Threat Program. However, the agency recognized in a June 2022 internal memo that it did not have a formalized independent assessment element within the program. The memo stated that the Insider Threat Program was working with DOE's Office of Enterprise Assessments to address the requirement for oversight compliance reviews.
- **Monitoring user activity on all classified networks**. Under the "monitor user activity on networks" topic area, minimum standards require that insider threat programs include the technical capability to monitor user activity on all classified networks.[28] According to DOE officials, the Insider Threat Analysis and Referral Center has not met full user activity monitoring coverage requirements on all classified networks, but has processes for addressing concerns on unmonitored classified networks should an event be detected by other means. Furthermore, DOE officials said that they have not identified the total number of DOE's stand-alone classified networks, which leaves them unaware of the extent to which the Insider Threat Program falls short of minimum standards for user activity monitoring. DOE officials said that they would like to identify the remaining classified networks. In

[27]U.S. Department of Energy, Office of Safeguards and Security Assessments, Office of Enterprise Assessments, *Special Assessment of the Department of Energy's Insider Threat Program.*

[28]As defined by the Committee on National Security Systems Directive 504, user activity monitoring is "the technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information in order to detect insider threats and support authorized investigations." According to the National Insider Threat Task Force, user activity monitoring is a significant information source for insider threat programs. User activity monitoring solutions identify, analyze, and contextualize anomalous behaviors within the information technology environment.

addition, DOE officials plan to increase monitoring coverage to all unclassified networks by 2027.

In addition to the four unmet minimum standards identified by the Director of National Intelligence, three additional minimum standards were found to be unmet through DOE's Office of Enterprise Assessments' review of DOE's Insider Threat Program in 2021.[29] The Office of Enterprise Assessments compared DOE Order 470.5 with the minimum standards and concluded that DOE's Insider Threat Program was in the establishment phase, the first of three phases for implementing minimum standards. Similar to the Director of National Intelligence's memo, the Office of Enterprise Assessments' assessment found that DOE had not fully implemented the minimum standards for insider threat awareness training and monitoring user activity on classified networks. The three additional minimum standards that the Office of Enterprise Assessment found to be unmet were:

- **Establishing procedures to access sensitive or protected information**. The Office of Enterprise Assessments' found that DOE Order 470.5 did not establish procedures for Insider Threat Program personnel to request access to categories of sensitive or protected information such as that held by special access, law enforcement, the Office of Inspector General, or other investigative sources, as is required by minimum standards in the "access to information" topic area. According to the Office of Enterprise Assessments' assessment, the challenges in access to information hampered the Analysis and Referral Center's ability to serve as the department's central information collection mechanism. DOE officials confirmed that challenges to accessing sensitive or protected information still remain for Insider Threat Program personnel.
- **Training program personnel in applicable civil liberty and privacy laws.** Under the "insider threat personnel" topic area, the minimum standards require agencies to ensure that the personnel responsible for implementing the Insider Threat Program are fully trained in topics such as applicable civil liberties and privacy laws, regulations, and policies. However, the Office of Enterprise Assessments found that DOE's Insider Threat Program senior official had not developed formal training to ensure that personnel associated with implementing the program were fully trained on legal issues, response actions,

[29]U.S. Department of Energy, Office of Safeguards and Security Assessments, Office of Enterprise Assessments, *Special Assessment of the Department of Energy's Insider Threat Program.*

handling of data and records, civil liberties, privacy, and investigative referral requirements. The assessment found that the Office of Insider Threat Program had endeavored to provide some training through venues such as site visits, although the training provided was informal. Several Local Insider Threat Working Group chairs confirmed that, as of June or July 2022, such training was being provided on an ad hoc basis to personnel at the site level. The extent of this training varied by site; for example, one Local Insider Threat Working Group chair reported providing biannual briefings to personnel about civil liberties issues, while another chair said that the site did not provide any training on civil liberties and privacy issues beyond what had been offered by the Office of Insider Threat Program.

- **Producing an annual report**. The senior official of an agency's Insider Threat Program must produce an annual progress report on the agency's insider threat programs, according to minimum standards in the "designation of senior official" topic area. The standard states that, at a minimum, the annual reports shall document annual accomplishments, resources allocated, insider threat risks to the agency, recommendations and goals for program improvement, and major impediments or challenges. However, the Office of Enterprise Assessments found that the Insider Threat Program's senior official had not submitted the required annual report to the Secretary of Energy since 2017. DOE officials told us that they had not released annual reports since the 2017 report because the program decided to wait until independent assessments of the Insider Threat Program were completed.[30] DOE officials also said that program staff did not have access to classified materials while working remotely during the COVID-19 pandemic, which contributed to some of the delay in annual reporting. Further, when we reviewed the 2017 Annual Report, it did not include information on resources allocated to the program, which is a minimum requirement.

[30]Specifically, DOE officials told us that they had been waiting for the DOE Office of Enterprise Assessments' report, which was issued in June 2021; the DOE Office of the Inspector General's assessment of the Insider Threat Analysis and Referral Center, which was issued in March 2023; and this review by GAO.

DOE Has Not Made Significant Progress in Addressing Recommendations from Independent Reviewers to Address Minimum Standard Requirements

Since 2015, the four independent reviewers have provided DOE with numerous findings and recommendations for its Insider Threat Program, many of which were intended to help the program achieve full operating capability. In our review of the independent assessments, we identified about 50 key findings and recommendations that reviewers had made to assist DOE with addressing gaps in the program. (For a summary of these findings and recommendations, see app. II.)

For example, the independent assessments included findings and recommendations related to employee training about insider threats and verification of training, which, as described above, are minimum standards that DOE has not yet met. In 2015, Carnegie Mellon University's Insider Threat Center recommended that DOE make enhancements to its insider threat awareness training process, stating that training completion should be required for all employees and that its completion should be tracked and verified. Similarly, in 2022, the National Insider Threat Task Force found that DOE had not yet taken steps to meet requirements for conducting and validating annual employee insider threat awareness training.

According to DOE officials, contractors, and independent reviewers, DOE has not yet addressed the findings and recommendations made about insider threat awareness training and verification of training. For example, several Local Insider Threat Working Group chairs we interviewed said that personnel at their sites receive some type of insider threat awareness training, but the type and extent of such training varies by site. Despite those local efforts, DOE officials told us that not all cleared employees and contractors are receiving insider threat awareness training that officials said would meet minimum standard requirements. Furthermore, DOE officials told us that, although they have an internal system to track training completion among employees and contractors, they may need to perform a data call every 6 to 12 months to collect training completion information from sites because contractors prefer to use their own local systems rather than DOE's system. Without implementing these recommendations from independent reviewers, DOE increases the risk that insider threat information could be improperly handled.

In general, independent reviewers we interviewed told us that DOE had not implemented many of their recommendations. For example, NASA officials told us in April 2022 that most of the findings and recommendations from their initial assessment made in 2015 still had not been addressed. In a presentation provided to DOE in September 2021, NASA noted that 16 of the 18 risks and challenges that NASA identified in

2015 remained unresolved. Further, NASA officials told us that they were unable to complete a full follow-on assessment of DOE's Insider Threat Program because DOE had failed to provide necessary documentation and to implement NASA's recommendations over the years, despite DOE's general agreement with them.[31] NASA officials also told us that they had an agreement with DOE to provide ongoing assistance to DOE's Insider Threat Program through 2025, but NASA cancelled its participation in the agreement in 2021 due to DOE's lack of responsiveness to NASA's findings and recommendations.

Similarly, Carnegie Mellon University reviewers told us that they have provided ongoing guidance to DOE on how to implement the recommendations they made to improve its Insider Threat Program and, although DOE has made some progress in training program personnel, the reviewers do not consider all of the recommended tasks as having been fully completed by DOE. In addition, the Director of National Intelligence confirmed in its March 2022 memo that DOE still had not addressed findings identified in its earlier assessments.

We were unable to determine the full extent to which DOE has taken action on the independent reviewers' findings and recommendations for its Insider Threat Program because DOE does not formally track its actions to implement the findings and recommendations against a comprehensive list of those findings and recommendations. DOE also has not submitted an annual report listing its annual accomplishments and goals for program improvement to the Secretary of Energy since June 2018. DOE officials told us that although they did not formally track recommendations made by independent reviewers, they used the recommendations available at the time to inform their *2017-2020 Strategic Plan for the Insider Threat Program.* DOE created a performance metrics dashboard to identify and track specific tasks that the program needed to complete to implement the strategic plan, although these tasks were not tied to any specific recommendations. According to the dashboard, DOE completed only 10 of 55 tasks to support the strategic plan through 2019. Officials told us that they stopped tracking performance on the tasks after 2019, about the time that the strategic plan was set to expire.

[31]According to NASA's interviews with program officials during its assessment, DOE officials said that documentation was not necessary because the Insider Threat Program staff already knew what they should be doing. Additionally, the officials said that increased documentation could potentially lead to increased accountability.

Since the 2017-2020 strategic planning effort, DOE has neither updated nor produced another plan to address recommendations nor set objectives and milestones for the program. According to DOE officials, efforts at drafting a successor strategic plan were interrupted when a senior security official instructed Office of Insider Threat Program officials to cease those activities in 2021. DOE officials also said that understaffing, as a result of a loss of personnel, affected strategic planning efforts. Officials said that efforts to fill some of those positions have been ongoing. They also said that the Office of Insider Threat Program is currently drafting a "Strategic Goals and Objectives" document, although DOE has not yet determined the timeline for completing that document.

Standards for Internal Controls in the Federal Government state that management should remediate internal control deficiencies on a timely basis.[32] For example, management could ensure that (1) identified deficiencies are corrected and (2) improvements are produced or (3) demonstrate that the findings and recommendations do not warrant management action. Further, the minimum standards require agencies to submit annual reports that document annual accomplishments and recommendations and goals for program improvement, among other things. Without taking steps to formally track findings and recommendations from independent assessments, documenting actions it has taken to implement them, and including those actions in its annual reporting on the program required by the minimum standards, DOE cannot fully ensure that identified program deficiencies and vulnerabilities have been addressed. DOE also cannot demonstrate that it is making substantial progress toward achieving a fully operational Insider Threat Program capable of effectively managing insider threats.

Multiple Factors Have Prevented DOE from Fully Implementing Its Insider Threat Program

We identified four factors that have prevented DOE from fully implementing its Insider Threat Program, which ultimately places DOE at greater risk of future insider incidents. Specifically, we found that DOE has not

1. effectively integrated Insider Threat Program responsibilities;
2. managed insider risk from a department-wide level;

[32]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 9, 2014).

3. established requirements to ensure that contractors consistently implement the Insider Threat Program at DOE sites; and
4. identified and assessed the human, financial, and technical resources needed to achieve full operating capability.

DOE Has Not Effectively Integrated Insider Threat Program Responsibilities

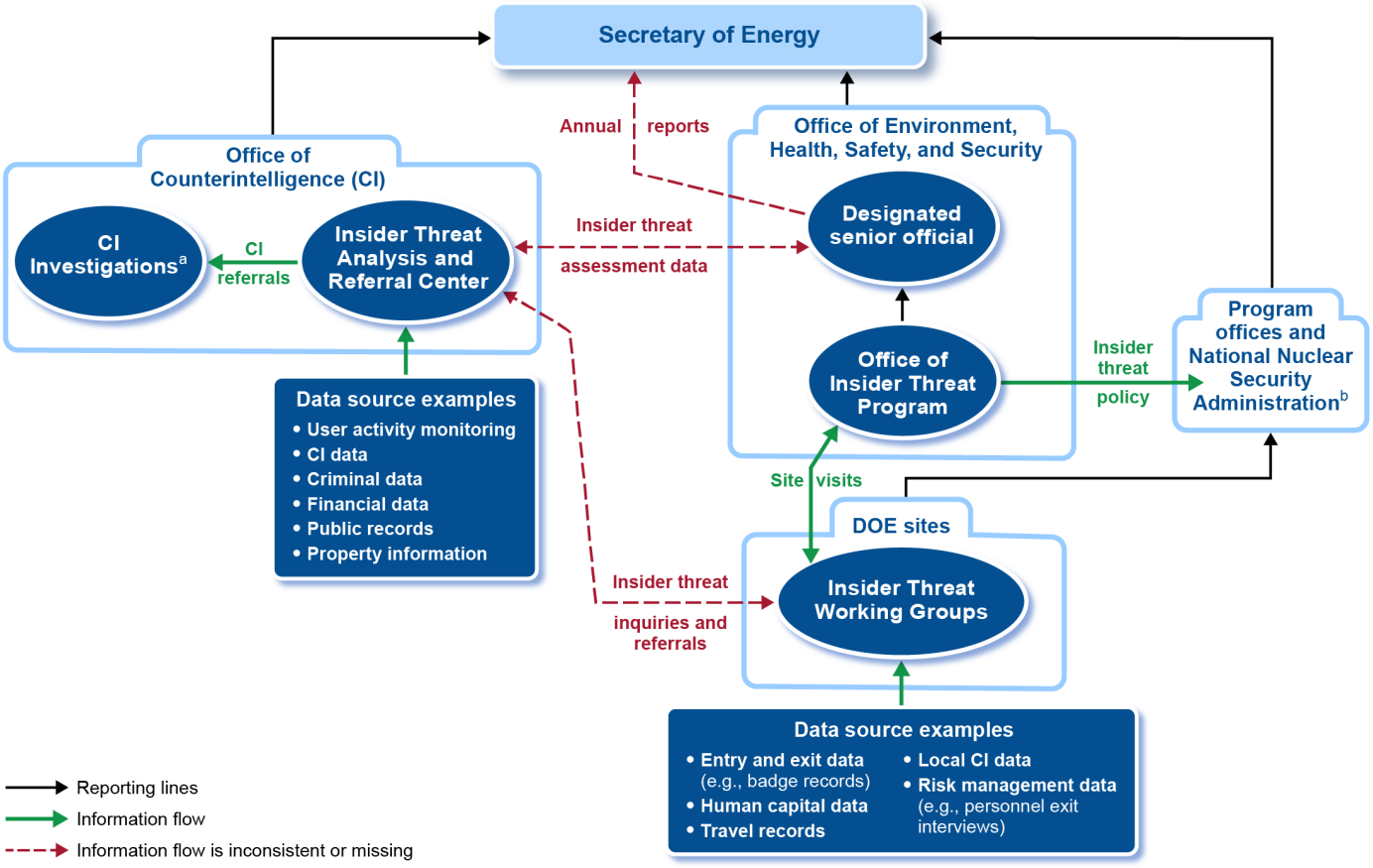
DOE has not effectively integrated Insider Threat Program responsibilities, as called for by the National Insider Threat Task Force and by the agency's own plans. Specifically, the minimum standards state that the designated senior official shall be responsible for establishing a process to gather, integrate, and centrally analyze and respond to all information indicative of a potential insider threat. The 2017 *Insider Threat Guide* further states that agencies should establish processes to centrally manage all insider threat response actions, in order to ensure that all necessary stakeholders have appropriate situational awareness, involvement, and oversight.[33] Likewise, DOE's 2014 *Insider Threat Program Implementation Plan* outlined a programmatic framework that was intended to implement a coordinated, well-functioning, and centrally managed Insider Threat Program.[34]

However, DOE subsequently divided significant program responsibilities between two offices by selecting a designated senior official from within the Office of Environment, Health, Safety, and Security, while retaining the Analysis and Referral Center within the Office of Intelligence and Counterintelligence. The implementation plan stated that the Analysis and Referral Center was to be activated under the Office of Intelligence and Counterintelligence only on a limited basis. However, this center continues to operate under the Office of Intelligence and Counterintelligence, largely independently and without oversight from the senior official, according to DOE officials. Figure 6 shows how the information is supposed to flow within DOE's Insider Threat Program and areas where information is not flowing between organizations, as originally intended.

[33]National Insider Threat Task Force, *Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards.*

[34]U.S. Department of Energy, *Insider Threat Program Implementation Plan* (August 2014).

Figure 6: Flow of Information through DOE's Insider Threat Program



Source: GAO analysis of Department of Energy (DOE) documents and interviews. | GAO-23-105576

Note: In addition to the entities depicted, DOE's Insider Threat Program has an Executive Steering Committee that includes senior management representation from the Office of Counterintelligence; the Office of Environment, Health, Safety, and Security; and the National Nuclear Security Administration, among others. The Executive Steering Committee meets quarterly to discuss issues related to DOE's Insider Threat Program, according to DOE officials.

[a]CI Investigations makes referrals to counterintelligence personnel at DOE sites, as appropriate.

[b]Program offices include the Office of Environmental Management, Office of Nuclear Energy, and Office of Science.

DOE Order 470.5 directs the Insider Threat Program senior official—who is located in the Office of Environment, Health, Safety, and Security—to oversee the entire Insider Threat Program. However, the Office of Counterintelligence has operational control over the Analysis and Referral Center because it provides the facilities, funding, and personnel to

operate that capability. DOE officials in those offices and the Office of Enterprise Assessments said that this bifurcated management structure has prevented the flow of insider threat information to the senior official.

For example, DOE officials told us that the Insider Threat Program and designated senior official do not always have access to information in the Analysis and Referral Center if, for example, an authorized decision maker determines that access to that information should be restricted to protect the integrity of a potential or ongoing counterintelligence investigation. As stated in the Analysis and Referral Center's approved procedures, all insider threat assessments and referrals are to be documented within the Counterintelligence Portal, a system of records utilized by the Analysis and Referral Center. Officials from the Office of Intelligence and Counterintelligence told us that access to the Counterintelligence Portal is not needed for the operation of the Insider Threat Program and that counterintelligence investigative information should not be provided to the Insider Threat Program.

However, in a March 2023 report, DOE's Office of Inspector General found that the senior official lacked access to referrals from the Analysis and Referral Center.[35] The Inspector General also found that the Analysis and Referral Center and the senior official did not consistently or proactively collaborate regarding critical threat information, including insider threat risks and program challenges, although the Analysis and Referral Center was required to do so, per the agency's procedures. Consequently, the Inspector General recommended that DOE ensure that the senior official receives insider threat information proactively and consistently from the Analysis and Referral Center and other relevant offices. DOE concurred with the recommendation and said that the agency plans to provide the senior official with access.

The National Insider Threat Task Force also found, based on several assessments dating back to 2016, that DOE's decision to divide program responsibilities between two offices created challenges for the program. In a memo to the Secretary of Energy in March 2022, the Director of National Intelligence concluded that DOE's bifurcated Insider Threat Program structure put the agency at greater risk for insider threats and precluded DOE from achieving a fully operational program.

[35]U.S. Department of Energy, Office of Inspector General, DOE-OIG-23-15, *Review of the Department of Energy's Insider Threat Analysis and Referral Center* (Washington, D.C.: Mar. 2023).

DOE has acknowledged that the designated senior official in the Office of Environment, Health, Safety, and Security has faced challenges in implementing a centrally managed program. In a June 2022 memo to the Deputy Secretary, the designated senior official and the Director of the Office of Intelligence and Counterintelligence noted that the Office of Environment, Health, Safety, and Security does not have organizational authority to manage DOE field elements (such as the eight nuclear security enterprise sites), which limits its ability to execute decisions and centrally manage the Insider Threat Program.

DOE has received multiple recommendations to move the senior official to a dedicated office outside of the security and counterintelligence offices, with a direct reporting line to the Secretary. For example, in 2015, as part of its assessment, NASA officials interviewed stakeholders across DOE who said that the senior official lacked sufficient ability to direct departmental components. It was the consensus view of the interviewees that the Insider Threat Program should be elevated to the Office of the Secretary. Similarly, in a March 2022 memo to the Secretary of Energy, the Director of National Intelligence noted that an effective program is not subordinate to either security or counterintelligence programs, but is a separate effort aligned with all organizational resources. Consequently, the Director of National Intelligence recommended that DOE operate its Insider Threat Program as a stand-alone component. In addition to those specific recommendations, the National Insider Threat Task Force's *Insider Threat Program Maturity Framework* states that mature insider threat programs should exist as a dedicated effort.

According to DOE officials, DOE senior leadership has considered the option of creating a dedicated Insider Threat Program at the Secretary level. However, in February 2023, the Secretary decided that the senior official would remain within the Office of Environment, Health, Safety, and Security. In August 2013, DOE established the first senior official as the Director of the Office of Security within the Office of Environment, Health, Safety, and Security. DOE has reassigned the senior official three times since 2013, each time assigning that position within the Office of Environment, Health, Safety, and Security. Specifically, in 2014, DOE reassigned the senior official to the Director of the Office of Corporate Security Strategy. In 2019, DOE reassigned the senior official one level higher within the Office of Environment, Health, Safety, and Security to the Deputy Associate Under Secretary for Security. In February 2023, DOE again reassigned the senior official one level higher in that office, to the Director of the Office of Environment, Health, Safety, and Security.

According to DOE senior leadership, the February 2023 reassignment of the senior official will be the first step in a series of changes to the program, including an update to DOE Order 470.5 to clarify roles and responsibilities. It is not yet clear what the scope of these program changes will be. However, reassigning the senior official to a higher level within the same office alone does not address the bifurcation of responsibilities between the two key offices. The February 2023 memorandum designating the senior official for the Insider Threat Program states that the senior official will encourage and facilitate collaboration but does not specify how that is to be accomplished. Without better integrating insider threat responsibilities between the Office of Environment, Health, Safety, and Security, and the Office of Intelligence and Counterintelligence, and ensuring that the senior official has the ability to provide central oversight and direction of all aspects of the program, DOE's Insider Threat Program will continue to face significant challenges that preclude it from having an effective or fully operational program.

DOE Has Not Managed Insider Risk at a Department-wide Level

DOE has been unable to overcome organizational barriers to centrally managing risk because the Secretary has not ensured a single, department-wide approach to managing insider threat risks. Rather than managing insider risk across all of these elements at the department level, as outlined in its strategic plan, DOE has delegated risk management to the individual program and site level.

First, DOE has many programs focused on managing risks associated with insider access that have their own processes in place, creating organizational silos that limit the ability to centrally manage insider risk. In its 2017 Annual Report, the Insider Threat Program stated that the department's extensive diversity across disciplines and the organizational structure that developed over the years created a substantial challenge for implementing the program at a department level.[36] The report further noted that the agency's decentralized structure had fostered the development of organizational barriers in the form of program office-specific processes, procedures, and systems that have significantly limited the agency's ability to manage department-wide security risk and that breaking down these organizational barriers would be challenging.

Second, DOE's operations are spread across multiple federal field offices and sites that are managed and operated by several different contractors.

[36]U.S. Department of Energy, *Insider Threat Program 2017 Annual Report.*

DOE has communicated that sites are responsible for managing the risk to their operations locally. For example, in a June 2022 memo to DOE senior leadership, the Insider Threat Program senior official stated that insider threat risk management resides at the site level. Similarly, a chair of a Local Insider Threat Working Group at a national laboratory told us that the Insider Threat Program has communicated to the working groups that contractors own the insider risk for their operations.

However, DOE previously identified that the Insider Threat Program would need to be managed at the department level to be successful. Specifically, under Strategic Goal 1, the DOE Insider Threat Program's *2017-2020 Strategic Plan* stated that the agency needed to enable the management of the program from a department level to effectively exercise DOE-wide initiatives and to leverage resources. The plan stated that success would ultimately be realized when the Insider Threat Program had a well-defined role, clear scope, and the full support and cooperation of all existing programs across the DOE complex that can help address the risks posed by individuals.

In addition, DOE identified that the program would need to leverage and exhibit the relationship between the program's senior official and the Secretary of Energy. Specifically, the plan stated that the President has directed the Secretary to actively execute an Insider Threat Program, and the Secretary is the sole official within the department that has the authority over all program elements. Therefore, the program needed to work to ensure that stakeholders were aware of the designated senior official's duty to carry out the program's responsibilities on the Secretary's behalf.

DOE subsequently developed a strategy to help overcome organizational barriers and better manage insider risk in a centralized, department-wide manner. In the strategic plan, DOE identified performance objectives that included redefining the role of the Insider Threat Program and exhibiting the relationship between the designated senior official and the Secretary of Energy. However, DOE did not complete the six tasks it intended to undertake in support of that strategy. DOE officials told us that they stopped tracking progress against the *2017-2020 Strategic Plan* as of 2019. According to the program's strategic plan performance tracker, tasks that were not completed included (1) updating DOE Order 470.5, (2) updating the Insider Threat Program implementation plan, and (3)

preparing a memorandum for the Secretary to sign that outlines further support for the program.[37]

Executive Order 13587 states that agency heads are responsible for implementing their respective insider threat programs. Officials from the Office of the Director of National Intelligence and the National Insider Threat Task Force explained that Executive Order 13587 places ultimate responsibility for managing insider threat risk on the agency head. Likewise, the *2017 Insider Threat Guide* states that agencies that are inherently hierarchical or regionally dispersed are at greater risk of experiencing gaps in coverage and that agencies should not assume that a subordinate unit or a geographically distant organization has its own Insider Threat Program.[38]

Because agency heads are ultimately responsible for insider threat risk to the agency, DOE senior leadership is expected to play a key role in shaping the program's approach to risk management. The *Guide to Accompany the National Insider Threat Policy and Minimum Standards* states that successful insider threat programs receive strong, personal, and visible support from the agency head and that leadership endorsement of the program is greatly enhanced when agency leaders lend their name and image to workforce communications about the program. In its 2017 annual report, DOE's Insider Threat Program stated that active and visible leadership endorsement would greatly enhance awareness of the program and would drive the development of a positive security culture.

In February 2023, the Secretary of Energy directed the designated senior official to integrate DOE's many capabilities into a single, comprehensive, risk management framework. DOE's Insider Threat Program had previously set this goal in its *2017-2020 Strategic Plan*, as described above. However, according to independent reviewers, organizational barriers and a lack of support from DOE senior leadership had prevented the designated senior official from carrying out the official's authorities. For example, according to its March 2022 memo to the Secretary of

[37]In February 2023, the Secretary of Energy issued a memorandum stating that the heads of all departmental elements, sites, and field offices were charged to render appropriate support to the designated senior official to integrate DOE's many capabilities into a single, comprehensive, risk management framework.

[38]National Insider Threat Task Force, *Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards.*

Energy, the Director of National Intelligence found that the designated senior official lacked support throughout the department to establish a dedicated Insider Threat Program.[39]

Another independent review team we spoke with observed that DOE senior leadership has been unreceptive to addressing the "cultural stovepipes" in the program's structure and that program officials were hesitant to carry out the authorities provided in DOE's Insider Threat Program order because of a lack of organizational support for a stronger role for the program. Without the Secretary's ongoing involvement to ensure that the Insider Threat Program achieves a department-wide approach to risk management, DOE will likely continue to manage insider risk locally in a decentralized way without effective management of department-wide risk, increasing the possibility of gaps and inconsistencies in risk management across the agency.

DOE Has Not Established Specific Requirements for Contractors' Insider Threat Program Implementation

Local Insider Threat Working Groups at the eight sites in the nuclear security enterprise are comprised mainly of contractors, according to the chairs of those groups. DOE Order 470.5—which applies to NNSA—requires contractors to provide data, information, systems, and other support to the program, as detailed in their contracts, but does not provide further details about how contractors are to fulfill that requirement.[40] The DOE order does not specify, for example, what data should be shared or when, with whom, or how it should be shared. The order also requires DOE program and staff offices, and NNSA, to provide direction to all contractors regarding their Insider Threat Program responsibilities; however, DOE has not established clear and specific responsibilities for the contractors.

Per DOE Order 470.5, the Office of Counterintelligence is responsible for establishing and providing guidance to the Local Insider Threat Working Groups, and the DOE program offices and NNSA are responsible for managing employees and contractors at the sites. To assist with developing and implementing effective Local Insider Threat Working Groups, the agency produced a technical standard with more detailed

[39]Director of National Intelligence, *National Insider Threat Task Force Assessment of the Department of Energy's Insider Threat Program Pursuant to Executive Order 13587 and the National Insider Threat Policy and Minimum Standards* (Washington, D.C.: Mar. 8, 2022).

[40]Of the eight sites we reviewed, Sandia National Laboratories was the only site that did not incorporate DOE Order 470.5 into its management and operating contract.

guidance, including that working groups should inform the Analysis and Referral Center as soon as possible of local insider threat issues.[41] However, that guidance is voluntary for sites to implement and does not establish requirements for contractors because it is not included as part of DOE and NNSA sites' management and operating contracts. Some chairs of the Local Insider Threat Working Groups we interviewed confirmed that their sites' management and operating contracts do not include the technical standard.

In part because of this lack of requirements, representatives from Local Insider Threat Working Groups told us that their level of interaction with the Analysis and Referral Center varied, and some groups have made few, if any, reports to the Insider Threat Program directly. According to the chair of one working group, the site does not report anything directly to the Analysis and Referral Center. Another working group chair told us that there is no dedicated system of records to report information to the Insider Threat Program. The chair said that noncounterintelligence information is not reported to the Insider Threat Program because it is not allowed in the counterintelligence portal that the Analysis and Referral Center uses. Instead, multiple, separate local data systems store insider threat information, depending on the type of incident, such as within human capital data systems for human capital-related incidents, according to the chair.

The DOE Office of Inspector General's March 2023 report also identified this issue, stating that the Analysis and Referral Center was not consistently receiving information from the Local Insider Threat Working Groups.[42] The Inspector General found that contractors did not provide information to the Analysis and Referral Center due to the fear of losing the contract. Consequently, the Inspector General recommended that DOE ensure that the Analysis and Referral Center receive threat information from the Local Insider Threat Working Groups and that DOE implement cross-organizational communication with the local working groups to ensure that referrals are addressed. DOE agreed with both recommendations and said that the senior official will work with the Office of Intelligence and Counterintelligence to address these issues.

[41]U.S. Department of Energy, DOE-STD-1227-2017, *DOE Technical Standard: Local Insider Threat Working Group Structure, Roles, and Response Actions* (Washington, D.C.: Mar. 2017).

[42]U.S. Department of Energy, Office of Inspector General, DOE-OIG-23-15.

The Insider Threat Program acknowledged these communication challenges in its 2017 annual report. The report stated that without established communication between the program's stakeholders, the risk that decision makers would not have all available information would continue to be a major concern for the program. Furthermore, the resulting information gaps could allow a potential insider threat to continue to develop undetected. More recently, in a March 2022 memo to the Secretary of Energy, the Director of National Intelligence noted that the lack of coordination between DOE headquarters and the sites created shortcomings in the ability of the Insider Threat Program to proactively counter insider threats throughout the agency. Without establishing contractors' responsibilities in the contract or the related requirements document, DOE cannot ensure that threat information is flowing between the sites and the program or ensure that potential insider threat incidents are being addressed.

DOE Has Not Identified or Assessed the Resources It Needs to Achieve a Fully Operational Insider Threat Program

DOE was required to identify all departmental resources that support the Insider Threat Program but has not yet done so. Specifically, DOE Order 470.5 and the minimum standards require DOE's Insider Threat Program to provide the Secretary of Energy with recommendations on the resources the agency needs to support the program. For example, DOE Order 470.5 directs program stakeholders to identify departmental resources to support the Insider Threat Program and provide this information to the Insider Threat Program Working Group.[43] However, this has not occurred because, according to DOE officials, the current senior official has not asked for, nor have program stakeholders provided, information on such resources. DOE officials also said that the Insider Threat Program Working Group has not met since at least 2018.

In its 2017 Annual Report, DOE stated that in 2015 it began an effort to identify the resources and capabilities necessary to accomplish the Insider Threat Program's mission. Accordingly, in its 2017-2020 strategic plan, the Insider Threat Program had set a performance objective, which included six tasks, to identify all current programs and processes that could be leveraged to address insider threats. However, as with many of

[43]According to DOE Order 470.5, the Insider Threat Program Working Group includes representation from offices with key responsibilities for the program. The working group is to provide a forum to address cross-organizational issues and support the senior official by, for example, drafting the annual report and providing it to the Executive Steering Committee for review.

its other efforts related to the strategic plan, DOE did not complete any of the six tasks to support this performance objective through 2019.[44]

Furthermore, Insider Threat Program officials said that they do not know whether DOE components have sufficient human, financial, and technical resources to support the Insider Threat Program because the program stakeholders have not worked together to assess whether existing funding is sufficient to meet needs. DOE Order 470.5 directs several DOE components to provide funding and technical resources to support the program.[45] However, only two DOE components have budgeted resources to provide for program-specific functions, according to DOE officials. Specifically, DOE budget documentation shows the average budgets for fiscal years 2018 to 2022 included

- $3 million for the Office of Insider Threat Program funded through the Office of Environment, Health, Safety, and Security, of which $1.5 million was used for contractor support for tasks including program administration, according to DOE officials;[46] and
- an additional amount to operate the Analysis and Referral Center, funded through the Office of Counterintelligence.[47]

However, those two line items do not account for staffing, analytic, and technology resources used across the agency to address insider threats and support the program. According to DOE officials, other DOE components have contributed human and financial resources through their own budgets to support the Insider Threat Program. However, those

[44]As mentioned previously, DOE stopped tracking progress against performance objectives after 2019, according to the Insider Threat Program's performance metrics dashboard and DOE officials.

[45]DOE Order 470.5 requires the following DOE components to provide funding and technical resources: (1) Office of Intelligence and Counterintelligence; (2) Office of Environment, Health, Safety, and Security; (3) Office of the Chief Information Officer; (4) Office of the Chief Human Capital Officer; (5) DOE program and staff offices; and (6) NNSA.

[46]In fiscal year 2022, DOE requested a 50 percent reduction in the budget for the Office of Insider Threat Program—to a total request of $1.5 million—in order to reallocate funding for security, suitability, and credentialing activities to the security operational support budget. However, under a continuing resolution, the fiscal year 2022 budget remained at $3 million. In its fiscal year 2023 request, DOE again proposed a decrease to reallocate funding for the same purpose—this time reducing the Insider Threat budget request by 66 percent, to $1 million.

[47]The exact amount of funding is in the budget of the Office of Intelligence and Counterintelligence, which is sensitive information.

offices do not report this information to the senior official, and they have not received specific funding to cover those responsibilities. For example, according to DOE officials and representatives of Local Insider Threat Working Groups we spoke with, working groups have received no dedicated funding to implement the program locally. Chairs of the local working groups said that the working groups depend on other existing program budgets—such as for security or counterintelligence activities—to fund their efforts, an arrangement that one working group described as an "unfunded mandate." Some working group chairs told us that they could use more resources to improve insider threat response activities, while other working group chairs said that current funding was generally sufficient. However, according to representatives from one of the independent review teams we interviewed, DOE has not requested more resources for addressing insider threats because it does not know what it needs. The reviewers said that, if given more resources, DOE would not know how to allocate them.

At least one DOE component has assessed that it needs additional resources to achieve compliance with program requirements and federal minimum standards. Specifically, an official from the Office of Counterintelligence said that the Analysis and Referral Center needs an additional $50 million to acquire software licensing and information technology hardware, and $5 million to hire an additional 20 analysts over a 5-year period to achieve compliance with minimum standards for user activity monitoring on classified networks and to cover all unclassified networks.[48] The minimum standards do not require coverage of unclassified networks, but the National Insider Threat Task Force recommends such coverage in its *Insider Threat Program Maturity Framework.* However, officials from the Office of Counterintelligence and Insider Threat Program stated that the designated senior official has not advocated for these resources because the Analysis and Referral Center is funded from the Office of Counterintelligence's budget, and the senior official does not have control of that budget.

According to the National Insider Threat Task Force's 2017 *Insider Threat Guide*, the senior official should be the primary advocate within the agency for program resources and for overseeing program resource

[48]A cost breakdown provided by the user activity monitoring contractor showed three pricing options over a 5-year period, including software, hardware, and staff: (1) approximately $40 million to cover 20,000 users, (2) approximately $54 million to cover 50,000 users, and (3) approximately $68 million to cover 100,000 users.

distribution across the entire agency.[49] Additionally, according to the guide, the senior official should look across all initiatives that comprise the program to advocate for mission-critical program requirements and to make informed recommendations to the agency head regarding resource trade-offs. Furthermore, according to the National Insider Threat Task Force's *Insider Threat Program Maturity Framework*, mature insider threat programs should have a dedicated program budget line item that provides for the staffing, analytic, and technology assets necessary to enable the program to maintain and improve effectiveness in fulfilling its objectives.[50]

The National Insider Threat Task Force has produced a cost planning tool for agencies to estimate the cost of standing up and operating an Insider Threat Program to meet the minimum standards under Executive Order 13587. However, DOE officials told us that it is challenging to estimate the costs to protect the agency from insider threats. For example, officials in NNSA explained that security measures are generally designed to address both external and internal threats, and it would be difficult to identify what portion of those costs specifically address insider threats. As stated above, each DOE component has been responsible for its own budget, and Insider Threat Program officials told us that they have not attempted to estimate program costs across the agency.

Unless Insider Threat Program stakeholders identify all departmental resources and work with the senior official to assess whether DOE components have the human, financial, and technical resources needed to support the Insider Threat Program, the senior official will be unable to provide recommendations to the Secretary on where resources should be allocated.

Conclusions

After taking initial steps in 2014 to set up an Insider Threat Program responsive to an executive order, DOE has yet to fully implement program requirements. Since 2015, several independent reviewers have provided DOE with recommendations and identified opportunities to improve its Insider Threat Program; however, DOE has not demonstrated substantial progress in implementing those recommendations. Without tracking recommendations and reporting annually on challenges and

[49]National Insider Threat Task Force, *Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards*.

[50]National Insider Threat Task Force, *Insider Threat Program Maturity Framework.*

accomplishments, as required, DOE cannot fully ensure that program deficiencies are being remediated in a timely manner.

DOE's inability to establish a fully operational Insider Threat Program resulted from several significant factors. First, the minimum standards, best practices, and DOE's own implementation plan have called for centralized management of insider threat response actions. However, the division of significant program responsibilities between program stakeholders has inhibited communication and program management, precluding DOE from having an effective or fully operational program. In addition, DOE continues to manage insider risk in a decentralized way because the Secretary has not fully ensured that the program has met its strategic goal for better managing insider risk at a department-wide level. DOE has taken the first step to addressing these long-standing issues by reassigning the designated senior official in February 2023 and directing that official to integrate DOE's capabilities into a comprehensive risk management framework. However, it is too early to assess how the remaining steps will be implemented.

Program progress is further hindered by a lack of clear and specific requirements for contractors' responsibilities, such as incident reporting. In addition, DOE has not conducted an assessment or recommended an allocation of program resources to ensure that all components are able to fulfill their responsibilities under the DOE order and minimum standards. DOE has relied largely on existing systems, processes, and funding streams for responding to insider threats at sites in the nuclear security enterprise. As a result, DOE has been unable to fully ensure that insider threat response actions at NNSA sites are consistent with program requirements and that the Insider Threat Program budget reflects the actual investment needed to ensure protection against insider threats across the agency.

Recommendations for Executive Action

We are making the following seven recommendations to DOE:

The Insider Threat Program senior official should develop a mechanism to track actions taken in response to findings and recommendations it receives from independent assessments. (Recommendation 1)

The Insider Threat Program senior official should resume annual reporting and include in those reports the actions the program has taken to address findings and recommendations it receives from independent assessments. (Recommendation 2)

The Insider Threat Program senior official should establish a process to better integrate insider threat responsibilities, ensuring that the senior official can centrally manage all aspects of the Insider Threat Program. (Recommendation 3)

The Secretary of Energy should ensure that the Insider Threat Program achieves a single, department-wide approach to managing insider risk. (Recommendation 4)

The Insider Threat Program senior official should work with DOE program offices and NNSA, in coordination with contracting officers, as appropriate, to ensure that contractors' specific Insider Threat Program responsibilities are clearly stated and consistently applied across the sites by, for example, reviewing and, if necessary, revising contract requirements to include responsibilities such as insider threat response actions. (Recommendation 5)

The Insider Threat Program senior official should work with Insider Threat Program stakeholders to identify all departmental resources that support the Insider Threat Program. (Recommendation 6)

The Insider Threat Program senior official should work with stakeholders to assess the program's human, financial, and technical resource needs and make recommendations to the Secretary on where resources should be allocated so that the program is positioned to achieve minimum standards. (Recommendation 7)

Agency Comments

We provided a draft of this report to DOE for review and comment. In its comments, reproduced in appendix I, DOE agreed with our recommendations and described plans to address them. DOE also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate committees, the Secretary of Energy, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-3841 or BawdenA@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 major contributions to this report are listed in appendix III.

Allison Bawden
Director, Natural Resources and Environment

Appendix I: Comments from the Department of Energy

Department of Energy
Washington, DC 20585

May 2, 2023

Ms. Allison Bawden
Director
Natural Resources and Environment
U.S. Government Accountability Office
441 G Street N.W.
Washington, DC 20548

Dear Ms. Bawden:

Thank you for the opportunity to review the Government Accountability Office (GAO) Draft Report, "*Nuclear Security: DOE Should Take Actions to Fully Implement Insider Threat Program* " (GAO-23-105576). The three enclosures to this letter provide the Department of Energy's consolidated response to the report's recommendations and a sensitivity review to determine if this report can be released to the public. Additionally, we have included specific comments to clarify the Department's layered security defense strategy and provide context for the Department's full capability for minimizing insider risks to the nuclear enterprise. The Department maintains programs that are specifically designed to avoid or minimize insider threats while capitalizing on longstanding protection measures against misuse of critical stockpile assets and resources.

If you have any questions or need additional information, please contact me at (202) 586-6740.

Sincerely,

Todd N. Lapointe
Director
Office of Environment, Health, Safety and Security

Enclosures

DOE Response to GAO Draft Report
NUCLEAR SECURITY: DOE Should Take Actions to Fully Implement Insider Threat Program (GAO-23-105576)

Recommendation 1: The Insider Threat Program senior official should develop a mechanism to track actions taken in response to findings and recommendations it receives from independent assessments.

Management Decision: Concur

Action Plan: The Department is conducting a review of referenced independent assessments and a thorough analysis of findings and recommendations to determine the current status and applicability for implementation. Conducting a comprehensive review allows the Department to develop an effective short-term strategy to address identified gaps in the current program and will enhance the ability to prevent and respond to insider threats.

The Insider Threat Program's Designated Senior Official (DSO) will ensure the development of a tracking mechanism for recommendations from independent assessments relating to the Insider Threat Program and monitor completion of appropriate corrective actions on a quarterly basis until the corrective actions are completed. This tracking mechanism will be in place no later than June 30, 2023.

Recommendation 2: The Insider Threat Program senior official should resume annual reporting and include in those reports the actions the program has taken to address findings and recommendations it receives from independent assessments.

Management Decision: Concur

Action Plan: An annual report is currently being drafted to address and identify the previous year's progress toward developing and implementing a viable program and will include updates and status for accomplishing recommendations identified through independent assessments of the program. Additionally, the Department's Insider Threat Program report will include annual accomplishments, allocated resources, identified threats, program goals, and any recognized challenges.

The annual report will be completed by July 31, 2023, and annually thereafter.

Recommendation 3: The Insider Threat Program senior official should establish a process to better integrate insider threat responsibilities, ensuring that the senior official can centrally manage all aspects of the Insider Threat Program.

Management Decision: Concur

Action Plan: The Secretary recently appointed the Director of the Office of Environment, Health, Safety and Security (EHSS) as the Insider Threat Program's Designated Senior Official (DSO) with a mandate to integrate and centrally manage the Department's Insider Threat Program. Consistent with the Secretary's direction, the DSO oversees the daily operation, management, strategic direction, accountability, and oversight of the Department's program. The Secretary conveyed a direction to Department leadership that the DSO will serve as the Departmental lead to articulate program requirements and facilitate collaboration. Additionally, the DSO will operate across functional lines on behalf of the Secretary to execute program requirements and integrate all mission tasks among program offices, headquarters, field offices and Local Insider Threat Working Groups (LITWGs), whether Federal, National Laboratory or contractor.

The DSO is currently leading a strategic review to identify any additional needed process changes. The DSO will complete the strategic review and identify needed changes by June 30, 2023.

Recommendation 4: The Secretary of Energy should ensure that the Insider Threat Program achieves a single, department-wide approach to managing insider risk.

Management Decision: Concur

Action Plan: In the recently issued designation memo the Secretary directed assistance from all Departmental stakeholders as the DSO integrates DOE's many capabilities into a single, comprehensive risk management framework.

The DSO will enhance collaboration and coordination between DOE/NNSA Program and Staff Offices, LITWGs, the Analysis and Referral Center within the Office of Intelligence and Counterintelligence, the Insider Threat Program Management Office within EHSS, Human Capital, the Chief Privacy Officer and other support programs in the development of the Insider Threat Program strategy. Additionally, NNSA recently established an Insider Threat oversight and liaison element within the Office of Defense Nuclear Security to assist the DSO in successfully implementing the Insider Threat Program throughout the Nuclear Security Complex.

The DSO is conducting an assessment of current strategies focused on reviewing the multidisciplinary governance group's composition to ensure that it consists of a well-rounded, diverse and versatile group of practitioners that bring a variety of perspectives, capabilities and backgrounds that can better address insider threat concerns. This initial assessment will be completed in May 2023.

The DSO will complete the strategic review and identify needed changes by June 30, 2023.

Recommendation 5: The Insider Threat Program senior official should work with DOE program offices and NNSA, in coordination with contracting officers, as appropriate, to ensure that contractors' specific Insider Threat Program responsibilities are clearly stated and consistently applied across the sites, by, for example, reviewing, and if necessary, revising contract requirements to include responsibilities such as insider threat response actions.

Management Decision: Concur

Action Plan: The Department's plan to update and revise the existing DOE Order 470.5, *Insider Threat Program*, will include specific responsibilities for senior officials, program stakeholders, program offices, and other relevant activities. The revised DOE Order will provide direction for contractors through a Contractor Requirements Document, consistent with the structure of DOE's Directives program. Updating the DOE order is a crucial step towards enhancing the effectiveness of the Insider Threat Program and will define clear roles and responsibilities while helping to ensure all stakeholders are aligned and working toward a common goal for mitigating insider threats. Ultimately, the success of the Insider Threat Program depends on the commitment and collaboration of all parties, federal employees, and contractors alike, and the update to the current order will provide a solid policy foundation.

Updates to the Order will commence by the fourth quarter of FY 2023 with the specific timeline and process coordinated with the Directives Review Board.

Recommendation 6: The Insider Threat Program senior official should work with Insider Threat Program stakeholders to identify all departmental resources that support the Insider Threat Program.

Management Decision: Concur

Action Plan: As the Department works to update its Insider Threat Program order, it will identify the necessary capabilities, resources, and other supporting elements. This process will require a thorough analysis of Departmental resources, human capital, and information technology/capabilities for implementing the program and will result in a robust and effective Departmental program that can detect and prevent insider threats.

Updates to the Order will commence by the fourth quarter of FY 2023 with the specific timeline and process coordinated with the Directives Review Board.

Recommendation 7: The Insider Threat Program senior official should work with stakeholders to assess the program's human, financial, and technical resource needs and make recommendations to the Secretary on where resources should be allocated so that the program is positioned to achieve minimum standards.

Management Decision: Concur

Action Plan: The process and analysis for completing an update to the Insider Threat Program order will identify the program's human, financial, and technical resource needs. After policy

requirements are set each departmental element will perform an impact assessment and implementation plan that will detail the added resources needed to implement. Program elements and NNSA, having governance and oversight responsibilities for specific insider threat functions, will communicate resource needs through established budget channels and will also inform the DSO of resource needs specific to Insider Threat Operations. By doing so, the program will be better positioned to allocate resources effectively and efficiently to address potential insider threats and improve the Department's implementation of program requirements to achieve compliance with the minimum standards. Additionally, the Executive Steering Committee, chaired by the DSO, will annually review program requirements identified in the revised order and provide recommendations for accomplishing national standards.

Appendix II: Prior Findings and Recommendations from Independent Assessments of the Department of Energy

We reviewed assessments of the Department of Energy's (DOE) Insider Threat Program from four independent reviewers that were issued between 2015 and 2022, following the program's establishment in June 2014. Where available, we also reviewed updates to the original assessments issued by the reviewer. These assessments compare DOE's Insider Threat Program to standards set by the National Insider Threat Task Force in the *National Insider Threat Policy and Minimum Standards* (minimum standards).[1] The program assessments described below comprise all those that have been completed by independent reviewers of DOE's Insider Threat Program.[2] Specifically, we reviewed assessments by the following:

- **Carnegie Mellon University's Insider Threat Center**. The university's Insider Threat Center conducts research through its federally funded research and development center, the Software Engineering Institute. According to university personnel, following a long-standing relationship with DOE, Carnegie Mellon University entered into an agreement with DOE beginning in 2013 to provide support as DOE established its Insider Threat Program. As part of its work, Carnegie Mellon University's center issued an assessment of DOE's Insider Threat Program in March 2015 in which it benchmarked DOE's program against minimum standards and the center's own best practices.[3] This assessment noted that because DOE was in the process of developing its Insider Threat Program, the analysis focused on the planning and implementation strategy being executed by DOE.
- **National Aeronautics and Space Administration's (NASA) Independent Verification and Validation Program**. DOE selected NASA's Independent Verification and Validation Program to review its Insider Threat Program because of its program evaluation expertise, according to NASA officials. NASA entered into an interagency agreement with DOE in 2015 for a two-stage evaluation process that consisted of an independent assessment and future support. Phase I

[1]National Insider Threat Task Force*, National Insider Threat Policy* and *Minimum Standards for Executive Branch Insider Threat Programs* (Nov. 21, 2012).

[2]In addition to the four reviewers described below, in March 2023 DOE's Office of Inspector General issued a more narrowly scoped assessment of DOE's Insider Threat Program, with a focus on the program's Insider Threat Analysis and Referral Center.

[3]Carnegie Mellon University, Software Engineering Institute, Computer Emergency and Response Team Insider Threat Center, *Insider Threat Program Evaluation: Department of Energy* (Mar. 2015).

commenced in the fall of 2015, and the first assessment report was issued in December 2015.[4] During this phase, NASA sought to assess DOE's program against requirements such as the minimum standards and DOE's implementation plan for the program. The NASA program conducted work until October 2021, when it terminated its second interagency agreement with DOE due to lack of information and responsiveness, according to NASA officials.

- **National Insider Threat Task Force.** The National Insider Threat Task Force is required to conduct independent assessments of the adequacy of agency programs to implement established policies and minimum standards. Office of the Director of National Intelligence entities, including the National Insider Threat Task Force and the National Counterintelligence and Security Center, conducted multiple assessments of DOE's Insider Threat Program from 2016 to 2020. We obtained and reviewed documents on those assessments, but we did not include findings and recommendations from those documents in our analysis because those documents are classified. Therefore, for our analysis, we use a March 2022 memo sent by the Director of National Intelligence to the Secretary of Energy, which summarizes the key findings and recommendations from previous assessments in an unclassified format.[5]
- **DOE's Office of Enterprise Assessments**. DOE's Office of Enterprise Assessments performs independent assessments for DOE senior leadership that report on whether national security material and information assets are appropriately protected and whether departmental operations provide for the safety of its employees and the public. According to DOE officials, the designated senior official for DOE's Insider Threat Program requested that the Office of Enterprise Assessments conduct a special assessment to evaluate the adequacy of the agency's Insider Threat Program policy requirements and implementation. The Office of Enterprise

[4]National Aeronautics and Space Administration Independent Verification and Validation Program, *Phase 1 Summary Report* (Washington, D.C.: Dec. 17, 2015).

[5]Director of National Intelligence, *Memo to the Secretary of Energy re: (U) National Insider Threat Task Force Assessment of the Department of Energy's Insider Threat Program Pursuant to Executive Order 13587 and the National Insider Threat Policy and Minimum Standards* (Washington, D.C.: Mar. 8, 2022).

Assessments issued its assessment in June 2021, in which it compared DOE Order 470.5 with the minimum standards.[6]

Table 1 summarizes findings and recommendations we identified and categorized from these four assessments and updates.[7] We categorized the findings and recommendations into the following nine categories:

1. *Training*. This category includes any findings or recommendations that address training for DOE employees or contractors on insider threat-related matters. Training includes both general insider threat awareness training offered to all cleared employees and contractors with security clearances, as well as specialized training offered to personnel implementing DOE's Insider Threat Program.
2. *Program structure*. This category includes any findings or recommendations that address how DOE's Insider Threat Program is organized, the roles and responsibilities of DOE personnel who participate in the program, and where the program and its senior official are positioned within DOE's organizational structure.
3. *Communication and collaboration*. This category includes any findings or recommendations that address how different elements of DOE's Insider Threat Program—for example, headquarters and the sites or the security and counterintelligence program offices—work together to implement the program and share information.
4. *Program scope*. This category includes any findings or recommendations that address what is covered by DOE's Insider Threat Program, such as the type of threats the program seeks to protect against and the assets it safeguards.
5. *Monitoring networks*. This category includes any findings or recommendations that address the Insider Threat Program's monitoring of classified or unclassified networks within DOE compared with requirements for such monitoring.
6. *Incident reporting and analysis*. This category includes any findings or recommendations that address the adequacy of DOE's Insider Threat

[6]U.S. Department of Energy, Office of Safeguards and Security Assessments, Office of Enterprise Assessments, *Special Assessment of the Department of Energy's Insider Threat Program* (Washington, D.C.: June 2021).

[7]We included in our review the eight key recommendations that Carnegie Mellon University's Insider Threat Center identified in its March 2015 assessment. The assessment included an additional 35 recommendations that provided more detail on the eight key recommendations; these additional recommendations are not counted in our table below.

Analysis and Referral Center's operations, insider threat incident reporting and analysis, and its referral process to other DOE entities.

7. *Program management*. This category includes any findings or recommendations that address the effectiveness of DOE's implementation of its Insider Threat Program, including meeting program requirements and providing necessary information for program oversight by independent reviewers.
8. *Contractor requirements*. This category includes any findings or recommendations that address the role that management and operating contractors play in implementing DOE's Insider Threat Program, the contents of relevant contractor requirement documents, and the extent to which contractors are following program guidance provided by DOE.
9. *Implementation plan*. This category includes any findings or recommendations that discuss the need for DOE to develop an implementation plan to ensure that its Insider Threat Program meets program requirements.

Table 1: Summary of Selected Findings and Recommendations from Independent Assessments of the Department of Energy's (DOE) Insider Threat Program, 2015–2022

Topic area	Number of findings and recommendations	Examples of findings and recommendations
Training	7	In March 2015, Carnegie Mellon University's Insider Threat Center made several recommendations to DOE about how it could improve training for Insider Threat Program personnel. For example, the center recommended that DOE should consider providing role-based training to different parts of the department that will interact with the Insider Threat Program. Carnegie Mellon University staff we interviewed in June 2022 told us that DOE has made significant progress on training its personnel and developed new training programs since the assessment was conducted. However, in March 2022, the Director of National Intelligence confirmed that DOE had not met minimum standards for annual employee insider threat awareness training or for validating insider threat awareness training.

Topic area	Number of findings and recommendations	Examples of findings and recommendations
Program structure	8	National Aeronautics and Space Administration's (NASA) Independent Verification and Validation Program identified several concerns about the structure of DOE's Insider Threat Program in December 2015, finding that there was confusion about roles and responsibilities, authority, and ownership of data and processes within the program. At the time, NASA noted that program staff believed that DOE's Insider Threat Program's Program Management Office and team should be organized at the Secretary of Energy level instead of being subordinate to DOE's counterintelligence and security programs. The Director of National Intelligence expressed a similar concern, recommending in March 2022 that the DOE Insider Threat Program should operate as a stand-alone component apart from the counterintelligence and security programs. In addition, multiple independent reviewers have identified the authority of the DOE Insider Threat Program's designated senior official as an issue that DOE needs to address. In December 2015, NASA's Independent Verification and Validation Program noted that DOE Order 470.5 gives the senior official authority for the Insider Threat Program but without direction over the programs that contribute to it. Furthermore, the Director of National Intelligence recommended in March 2022 that DOE should select a senior official that is vested with sufficient authority to ensure that all DOE Insider Threat Program resources are integrated and coordinated.
Communication and collaboration	6	Shortly after DOE's Insider Threat Program was established, Carnegie Mellon University's Insider Threat Center and NASA's Independent Verification and Validation Program identified the lack of communication and engagement at the DOE site level as impediments to the program. Carnegie Mellon University reviewers told us that DOE has taken steps since their findings were made in 2015 to establish Local Insider Threat Working Groups at DOE sites and obtain buy-in from site-level personnel. However, in June 2021, DOE's Office of Enterprise Assessments recommended that DOE should update DOE Order 470.5 to better reflect how information should be shared. In addition, the Director of National Intelligence recommended in March 2022 that DOE's Insider Threat Program should collaborate more closely with DOE's counterintelligence program, as well as with all security disciplines, including personnel security and information and cybersecurity.
Program scope	5	In December 2015, NASA's Independent Verification and Validation Program recommended that DOE should fully document the identification of what is within the scope of the Insider Threat Program and what falls outside its scope (i.e., risks, networks, sites, etc.). DOE's Office of Enterprise Assessments made a similar recommendation in June 2021, when it stated that the designated senior official of DOE's Insider Threat Program should determine the scope of the program by identifying what insider threats and associated departmental assets are to be addressed by the program.
Monitoring networks	5	In their 2015 assessments, Carnegie Mellon University's Insider Threat Center and NASA's Independent Verification and Validation Program both identified gaps in DOE's monitoring of user activity on its networks. NASA's assessment stated that to be truly effective, the DOE Insider Threat Program's Analysis and Referral Center needed to expand its monitoring and access to all networks. This issue is ongoing; the Director of National Intelligence found in March 2022 that DOE has not met minimum standards for monitoring user activity on classified networks.

Topic area	Number of findings and recommendations	Examples of findings and recommendations
Incident reporting and analysis	5	NASA's Independent Verification and Validation Program identified a number of concerns about incident reporting and analysis done by DOE's Insider Threat Analysis and Referral Center in its December 2015 assessment. For example, NASA's assessment found that there is limited feedback of how incidents are closed or addressed when identified by the Analysis and Referral Center and referred to the field offices.
Program management	4	Several independent reviewers identified program management issues that have affected DOE's Insider Threat Program. For example, NASA's Independent Verification and Validation Program found in December 2015 that the program's overall inability to provide consistent and documented data of what was needed and what had been collected had resulted in an inability to track information. In June 2021, DOE's Office of Enterprise Assessments also recommended that DOE should follow the approach of an agency that has achieved full operating capability—i.e., met all minimum standards—to better fulfill program requirements. Furthermore, in March 2022, the Director of National Intelligence reported that DOE has not met the minimum standard for internal oversight compliance.
Contractor requirements	3	In June 2021, DOE's Office of Enterprise Assessments' assessment of DOE's Insider Threat Program noted that contractors manage and operate the majority of DOE sites based on specific contract obligations, and the fulfillment of contract requirements often varies based on their program secretarial office direction and their uniquely established processes and systems. The office recommended that DOE update its insider threat policy, DOE Order 470.5, to include a contractor requirement that specifies performance goals and outcome-based requirements, when possible.
Implementation plan	2	In December 2015, NASA's Independent Verification and Validation Program recommended that DOE should fully document an overall action or project plan that includes an implementation schedule for the Insider Threat Program and assigns responsibility for the implementation process. DOE's program developed an initial implementation plan in 2014. However, according to DOE officials, the program shifted to following a strategic plan for 2017-2020—which has not been updated—without meeting all the milestones in the original implementation plan. In June 2021, DOE's Office of Enterprise Assessments recommended that the designated senior official of DOE's Insider Threat Program should develop an implementation plan with milestones to bring the department into full compliance with Executive Order 13587. Furthermore, the office recommended that DOE should update DOE Order 470.5 to mandate that DOE headquarters, field offices, and site contractors develop an implementation plan with Insider Threat Program milestones and report progress to the program's designated senior official at least annually in the required annual report to the Secretary of Energy.
Total	**45**	

Source: GAO analysis of documents from Carnegie Mellon University, DOE, the Office of the Director of National Intelligence, and NASA. | GAO-23-105576

Note: The assessment conducted by Carnegie Mellon University's Insider Threat Center includes 35 recommendations. However, for our analysis, we include only the eight key recommendations identified by the assessment because these recommendations effectively include all of the topic areas covered by the more detailed and technical 35 recommendations.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact:	Allison Bawden, (202) 512-3841 or BawdenA@gao.gov

Staff Acknowledgments:	In addition to the contact named above, Hilary Benedict (Assistant Director), Daniel Will (Analyst in Charge), Keya Cain, Antoinette Capaccio, Cindy Gilbert, Gwen Kirby, and Danny Royer made significant contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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