Safeguards and Security

Overview

The Office of Science (SC) Safeguards and Security (S&S) program is designed to ensure critical Federally-mandated security measures are in place to protect the array of government and national security assets, information, and data entrusted to SC. These assets are critical to accomplishing the SC mission of basic research in key scientific fields such as physics, materials science, computing, and chemistry, as well as fundamental scientific research related to energy and includes vital support for Executive Order 14363, *Launching the Genesis Mission,* and providing a secure artificial intelligence (AI) platform for sharing our Nation's scientific research.

Potential threats to SC high-consequence assets come from an array of evolving sources that the DOE's Office of Intelligence/Counterintelligence, National intelligence agencies, and local law enforcement agencies follow, to include transnational terrorists, domestic terrorists, criminals, disgruntled employees, malevolent insiders motivated for financial or ideological reasons, and foreign national visitors with the malicious intent of performing espionage. In response to an evolving threat landscape, the federal government and DOE recently revised several security policies to ensure critical assets remain protected. Implementation will continue to be executed through a risk-informed decision-making process that will facilitate capability expansion in the most consequential areas. An important factor contributing to an increase of potential threats at SC laboratories is the tremendous growth of local infrastructure bringing homes, schools, and commercial businesses close to laboratory boundaries.

The security measures employed at each of the 10 Science National Laboratories and three federal sites are based on National and DOE requirements. The requirements are solidified in DOE policies approved by the Secretary or Deputy Secretary of Energy and reflect the Department's acceptable level of risk. SC ensures these policies are formally incorporated in contracts at each of the SC sites, and Federal line management provides oversight to ensure implementation is cost effective and achieves the required level of security performance.

To counter security threats and support operations, the physical security program continually looks to decrease reliance on human-based protection services and leverage the latest security technologies and tactics, to include AI systems and software, to enhance program performance and effectiveness. Beginning in FY 2027, SC will implement an Artificial Intelligence (AI) for Operations initiative aimed at combining enhanced data collection and analysis with AI tools to streamline mission-critical functions and provide predictive, insight-driven information for enterprise risk management. SC's S&S program also provides funding for cybersecurity for the laboratories' information technology systems to protect SC mission systems, computers, networks, and data from unauthorized access and virtual incursion from many of these same threats.

The S&S program supports specialists in nuclear material control and accounting; advanced security systems and centralized alarm monitoring stations; classified and unclassified controlled information; personnel vetting, to include employees and foreign visitors; protective forces; and cybersecurity. Across the 10 laboratories and three SC federal facilities, there are nearly 550 physical security and 170 cyber professionals supporting the SC mission. Funding is vital to sustain the services of these security professionals, as approximately 90 percent of the physical security requirement is labor-based. The SC security workforce is responsible for the protection of over 20,000 acres, 1,500 buildings, and a combined laboratory workforce population exceeding 94,000 (including guest researchers, users, employees, etc.).

SC's S&S program is also incorporating emerging technology and security requirements to protect the scientific mission at each of the SC sites. These efforts require upcoming investments in AI to align with America's AI Action Plan and progressive cyber initiatives to support a wide range of Executive Orders. An increase in human capital investment and enhancements to logging, monitoring and identity credentialing and access

management system will be needed to support the Genesis Mission and the security of the American Science Cloud. This current profile will enable the SC program to continue to meet the most critical current requirements.

Highlights of the FY 2027 Request

The S&S FY 2027 Request for S&S is $202.5 million, which is $12.5 million above the FY 2026 Enacted level. The FY 2027 Request for Physical Security is $113.4 million and will support baseline compliance with federal standards and maintenance of a sustained secure Physical Security posture for current SC complex requirements. The increase to Cybersecurity program of $6.6 million will fully fund the Continuous Diagnostics and Mitigation reporting requirement ensuring compliance to the federal mandate. The FY 2027 Request will also provide initial support to SC's anticipated contributions to Cybersecurity for the Genesis Mission and initial implementation of security vetting practices that will protect the integrity of the Genesis platform. This budget will support annual labor rate increases and sustain security operations. The FY 2027 Request will support employment of nearly 550 physical security and 170 cybersecurity professionals. The FY 2027 Request will support the maintenance and replacement of the highest priority end-of-life security systems across the 13 SC laboratories and sites.

Description

The S&S program is organized into seven program elements:

1. Protective Forces
2. Security Systems
3. Information Security
4. Cybersecurity
5. Personnel Security
6. Material Control and Accountability
7. Program Management

Protective Forces

The Protective Forces program element supports security officers and security police officers that control access and protect S&S assets, along with their related equipment and training. Protective Forces at SC laboratories and facilities, and their coordinated efforts with federal and local law enforcement agencies, are our first line of defense against any violent attack against DOE personnel, contractors, and visitors. Activities within this program element include access control and security response operations as well as physical protection of the Department's critical assets and SC facilities, including critical facilities and data centers used to support the Genesis Mission. The Protective Force response and deployment configurations at SC laboratories reflect some of the most advanced tactical operator skills within the U.S. government (e.g., the armed security police officers protecting Building 3019 at ORNL), which are necessary due to the inherent consequences of protecting nuclear materials, critical program assets, and classified information. Maintaining these advanced tactical capabilities necessitates continuous, updated training to effectively align with DOE's evolving national security requirements. Additionally, the Protective Forces mission includes providing effective response to emergency situations, prohibited article inspections, security alarm monitoring, and performance testing of the Protective Force response to various event scenarios.

Security Systems

Detection and delay of potential threats at SC facilities is made possible by security systems that provide SC sites with advanced notification to save lives and protect DOE property, classified information, hazardous materials, and other national security assets. The Security Systems program element provides the backbone of the physical protection of Departmental personnel, material, equipment, property, and facilities. Systems currently deployed at SC sites include, but are not limited to, Homeland Security Presidential Directive 12 (HSPD-12) and local credentials, entry control points, fences, barriers, lighting, alarms, sensors, surveillance

devices, access control systems, and power systems. In addition, the continued use of AI-based technologies provides further enhanced performance with respect to sites' abilities to detect, identify, track, and classify physical security threats in real-time, to include people and vehicles, at and within the site perimeter (e.g., the advanced AI-based video analytics used at Laboratories such as Argonne National Laboratory and SLAC National Accelerator Laboratory).

Information Security

The Information Security program element provides support to ensure that sensitive and classified information is accurately, appropriately, and consistently identified, reviewed, marked, protected, transmitted, stored, and ultimately destroyed. Specific activities within this element include management, planning, training, and oversight for maintaining security containers and combinations, marking documents, and administration of control systems, operations security, special access programs, technical surveillance countermeasures, and classification and declassification determinations. In particular, the classification area of this program element has experienced a significant increase in the volume of work because of SC's growth in national security activities and federal requirements to digitize millions of pages of scientific working documents, which must first undergo a classification review (e.g., since 2021, classification reviews at ORNL have increased by 94 percent).

Cybersecurity

The Cybersecurity program element develops and maintains a comprehensive program for SC's 10 national laboratories and three federal sites. This program monitors numerous advanced persistent threats (APTs) that aim to disrupt critical missions and exfiltrate vital research and intellectual property across domains such as artificial intelligence, material science, high performance computing, and basic research. The risks posed by these APTs extend beyond mission disruption and intellectual property theft to include the potential compromise of Personally Identifiable Information (PII) belonging to federal and contractor personnel. The objectives of the Cybersecurity program element are to enable mission objectives and scientific endeavors, enhance the overall security posture through the adoption of advanced security designs, and provide consistent guidance and cybersecurity procedures. Furthermore, the Cybersecurity program element plays a crucial role in responding to cyber incidents by supporting incident management, prosecution, and investigation efforts related to cyber intrusions. It also facilitates disaster and incident recovery, as well as communication within the cybersecurity community. SC Cybersecurity is intrinsically aligned with the mission to secure the American Science Cloud under the Genesis Mission, which is intended to be the world's leading scientific platform for accelerating discovery, strengthening national security, and advancing energy innovation.

Personnel Security

The Personnel Security program element is critical to identification of predictors of potentially dangerous or destructive behavior at SC laboratories as well as evaluation of individuals accessing information shared in the Genesis Mission. This includes processes for employee suitability and security clearance determinations at each site to ensure that individuals are trustworthy and eligible for access to DOE facilities, IT networks, and classified information or material. This also includes the new Federally mandated requirements for continuous evaluations, which generates thousands of additional Federal adjudications on a monthly basis. Additionally, this program element addresses the process of vetting the uncleared contractor workforce that have physical and/or logical access to federal facilities, information, and personnel. This element also includes the management of security clearance programs, adjudications, security education, and awareness programs for Federal and contractor employees. The Personnel Security program element also manages the Human Reliability Program to ensure individuals who occupy positions affording access to certain materials, nuclear explosive devices, facilities, and programs meet the highest standards of reliability and physical and mental suitability. In accordance with 50 USC 2652 and DOE Order 142.3B, *Unclassified Foreign National Access Program*, the program processes, in collaboration with Office of Intelligence (IN) and Office of Environmental, Health, Safety, and Security (EHSS), the large number of foreign visitors that engage with the 10 Science

laboratories to mitigate Nation State information and intelligence collection efforts. This process includes, at a minimum, the completion of indices checks, with additional local vetting conducted when dictated by factors such as the facility being visited, the duration of the visit, and the science and technology involved.

Material Control and Accountability (MC&A)

The MC&A program element provides assurance that Departmental materials are properly controlled and accounted for at all times. The performance of this program element includes, but is not limited to, testing performance and assessing the levels of protection, control, and accountability required for the types and quantities of materials at each facility; documenting facility plans for materials control and accountability; assigning authorities and responsibilities for MC&A functions; and establishing programs to detect and report occurrences such as material theft, the loss of control or inability to account for materials, or evidence of malevolent acts.

Program Management

The Program Management program element functionally integrates and oversees the S&S Program, including Protective Forces, Security Systems, Information Security, Personnel Security, and MC&A to achieve and ensure appropriate levels of security are in place through performance assurance activities such as self-assessments, maintenance, and performance testing. The performance of this program element has direct involvement with the sites' Insider Threat Programs to deter, detect, analyze, respond to, and mitigate insider threat actions (such as espionage, sabotage, unauthorized disclosure, workplace violence, active shooter, etc.) by DOE federal and contractor employees. This program element also includes the performance of vulnerability and/or security risk assessments, which provides a technical basis for the integrated security program at the sites and the acceptance of any associated residual risk. Beginning in FY 2027, the Program Management program element will implement an Artificial Intelligence (AI) for Operations initiative aimed at combining enhanced data collection and analysis with AI tools to streamline mission-critical functions and provide predictive, insight-driven information for enterprise risk management. This initiative is aligned with America's AI Action Plan in that it will accelerate AI adoption in the federal government, enabling employee adoption of tailored tools that can be used to enhance the quality and accuracy of national laboratory oversight duties and proactively identify, mitigate, and respond to maintenance issues, security threats, and safety risks, resulting in cost and time savings and fewer disruptions to scientific and engineering innovation.

Safeguards and Security
Funding

(dollars in thousands)

	FY 2025 Enacted	FY 2026 Enacted	FY 2027 Request	FY 2027 Request vs FY 2026 Enacted
Safeguards and Security				
Protective Forces	57,732	57,428	59,645	+2,217
Security Systems	21,068	20,686	21,009	+323
Information Security	5,830	5,801	5,978	+177
Cybersecurity	82,497	82,497	89,097	+6,600
Personnel Security	10,553	10,680	11,118	+438
Material Control and Accountability	3,494	3,548	3,880	+332
Program Management	8,826	9,360	11,773	+2,413
Total, Safeguards and Security	**190,000**	**190,000**	**202,500**	**+12,500**

Safeguards and Security
Explanation of Major Changes

(dollars in thousands)

FY 2026 Enacted	FY 2027 Request	Explanation of Changes FY 2027 Request vs FY 2026 Enacted
Safeguards and Security **$190,000**	**$202,500**	**$12,500**
Protective Forces $57,428	$59,645	+$2,217
Funding maintains support for security officers and their required equipment, and at some sites, advanced armament specifically analyzed and required to combat advanced threats to our weapons grade nuclear materials. Additionally, funding supports training for these perishable skills, thereby ensuring the readiness of our security officers at all SC laboratories.	The Request will support current baseline security officer and equipment requirements. Also, funding will support training for the protective force to ensure the readiness of our security officers at all SC laboratories.	Funding will support expanding levels of operations and training for Protective Forces.
Security Systems $20,686	$21,009	+$323
Funding maintains support for the security systems in place as well as continued implementation of security modifications and enhancements that support the deterrence, sensing, and assessment of an array of threats to our range of assets.	The Request will maintain support for existing security systems. Security modifications and enhancements will continue on a priority basis.	Funding will address current operations. Additionally, funding will support the replacement of the highest priority end of life security systems across the 13 SC sites.
Information Security $5,801	$5,978	+$177
Funding maintains support for the personnel, equipment, training, and systems necessary to ensure the growing SC mission and associated sensitive and classified information is safeguarded at SC laboratories.	The Request will maintain support for current personnel, equipment, training, and systems.	Funding will support sustained levels for Information Security activities.

(dollars in thousands)

FY 2026 Enacted	FY 2027 Request	Explanation of Changes FY 2027 Request vs FY 2026 Enacted
Cybersecurity $82,497	$89,097	+$6,600
Funding supports investments in cyber infrastructure and cyber capability including new cyber tools, incident response enhancements, cyber workforce development, data protections, and protections for unique SC facilities and capabilities that cannot be protected with commercial tools. Additionally, the funding continues implementation of Executive Order 14028 requirements at both federal and Management & Operating sites to build out Maximum MFA, Maximum Encryption, Cloud Strategy/Security, Improved Logging and Supply Chain Management, Zero Trust Infrastructure, Secure Critical Software, Controlled Unclassified Information cyber protections, participate in the Department of Homeland Security Continuous Diagnostics and Monitoring program, build out Industrial Control Systems protections, and protect Government Furnished Equipment on foreign travel.	The Request will support investments in cyber infrastructure and cyber capability. The Request will continue implementation of Executive Order 14028 requirements at both federal and Management & Operating sites to continue current efforts to build out Maximum MFA, Maximum Encryption, Cloud Strategy/Security, Improved Logging and Supply Chain Management, Zero Trust Infrastructure, Secure Critical Software, Controlled Unclassified Information cyber protections, AI protections, AmSC under the Genesis mission, participate in the Department of Homeland Security Continuous Diagnostics and Monitoring program build out Industrial Control Systems protections, and protect Government Furnished Equipment on foreign travel.	Funding will support sustained efforts to continue implementing Executive Order 14028 requirements to include Zero Trust Infrastructure and additional scope of work involving the American Science Cloud under the Genesis Mission.
Personnel Security $10,680	$11,118	+$438
Funding continues support for processing of clearances and the vetting of uncleared personnel of the large workforce at SC laboratories as well as SC Headquarters security investigations. Also, funding supports the processing of the large number of foreign visitors that engage with the 10 Science laboratories, which is vital to thwarting known Nation State	The Request will support processing of clearances and the vetting of uncleared personnel at SC laboratories, multiple Office of Environmental Management laboratories as well as SC Headquarters. The Request will provide support to the processing of the large number of foreign visitors that engage with the 10 Science laboratories, which could exacerbate insider threat risks by	Funding will provide support for personnel security at increased overhead and inflation rates, and also the additional scope of work involving the American Science Cloud under the Genesis Mission.

(dollars in thousands)

FY 2026 Enacted	FY 2027 Request	Explanation of Changes FY 2027 Request vs FY 2026 Enacted
information and intelligence collection efforts.	impeding rapid investigative reviews and continuous evaluations. The request will also support vetting and authentication of personnel requesting access to the American Science Cloud.	
Material Control and Accountability $3,548	$3,880	+$332
Funding continues to support functions ensuring Departmental materials are properly controlled and accounted for at all times and to detect and report occurrences such as material theft, the loss of control or inability to account for materials, or evidence of malevolent acts.	The Request will maintain support functions ensuring Departmental materials will be properly controlled and accounted for at all times and to detect and report occurrences such as material theft, the loss of control or inability to account for materials, or evidence of malevolent acts.	Funding will provide support for MC&A activities at increased overhead and inflation rates.
Program Management $9,360	$11,773	+$2,413
Funding continues support for oversight, administration, analysis, and planning for security programs at SC laboratories and provides integration of all security elements and security procedures protecting SC Research missions. In addition, funding ensures all security programs and elements will continue to perform as designed through on-going testing and assurance activities.	The Request will maintain support for oversight, administration, analysis, and planning for security programs at SC laboratories and provides integration of all security elements and security procedures protecting SC Research missions. In addition, the Request will ensure all security programs and elements will continue to perform as designed through on-going testing and assurance activities. This Request will provide initial funding to an AI for Operations initiative aimed at refining AI use cases and piloting AI tools across national laboratory operations.	Funding will provide support for Program Management activities at increased overhead and inflation rates while beginning new work in support of AI for Operations.