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 entrusted to SC. These assets are vital 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.

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.

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 level of acceptable protection and risk. Failure to implement these requirements degrades security and increases National security risk, such as unauthorized access to facilities and information, and unauthorized use of weapons-grade special nuclear material and radiological materials. SC ensures these policies are formally incorporated in the contracts at each of the SC sites and Federal line management provides oversight to ensure implementation is cost efficient and achieves the required level of security performance.

Accomplishing the full scope of security operations to support the SC mission depends on providing physical security tools, processes, and cyber security controls that will mitigate current and future threats to the laboratories' employees, nuclear and special nuclear materials, classified and sensitive information, hazardous materials, mission essential functions and facilities, using risk-based decision processes. To counter these 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 artificial intelligence (AI) systems and software, to enhance program performance and effectiveness in addressing new and emerging threats. The SC 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.

Accomplishing the security mission is heavily reliant on SC sites employing security professionals in a wide range of technical security disciplines. The suite of security professionals at the sites includes specialists in nuclear material control and accounting; advanced security systems and centralized alarm monitoring stations; classified and unclassified controlled information handling and marking; personnel vetting, to include employees and foreign visitors; protective forces training and highly qualified security officers; a broad range of technical experts in varying cybersecurity disciplines; and security management and assurance. Across the 10 laboratories and three SC federal facilities, there are nearly 550 physical security and 170 cyber professionals supporting the SC mission. Congressional security direct funding is vital to sustain the services of these security professionals as approximately 90 percent of the physical security funding is currently labor based. The SC security workforce represents one of the most labor efficient workforces in DOE/NNSA based on the number of sites under the purview of SC (reference the DOE Security Crosscut). Additionally, across all of SC, the 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.). While the security workforce is efficient, it must also be postured to scale in the out-years in order to meet emerging requirements and the rapidly expanding scientific mission at each of the SC sites. The latter includes more assets, facilities, and a growing workforce. Based on projected increased costs for IT and Cyber related services and applications, along with mandated requirements for Zero Trust, CUI, the transfer of CDM (Continuous Diagnostics and Mitigation) costs from OCIO to SC, and the stand-up of a SOC (Security Operations Center) to support the Office of Science, current requirements also continue to increase for cybersecurity. The FY 2026 Request remains flat with the FY25 Enacted budget. This profile will enable the program to continue to meet current requirements but will inhibit development of innovative technology solutions and delay divestment of legacy systems and processes that could potentially realize savings in the future.

Highlights of the FY 2026 Request

The S&S FY 2026 Request for S&S is $190.0 million, which is flat with FY 2025 Enacted level. This budget will cover resource annual labor rate increases, and hence, the sustainment of the nearly 550 physical security professionals. The remaining balance will support the replacement of highest priority end of life security systems across the 13 SC laboratories and sites.

The FY 2026 Request includes $82.5 million in Cybersecurity to help address long-standing gaps in IT infrastructure, operations, and compliance to ensure adequate detection, response, protection, identification and recovery from cyber intrusions and attacks against the 13 SC laboratories and sites. The FY 2026 Request supports the implementation of requirements set forth by the administration and congress for Multi-Factor Authentication (MFA) where feasible, Encryption of data both at rest and in transit, Cloud Strategy/Security, Improved Logging, Supply Chain Management, and Zero Trust Infrastructure to address the continued attacks on our IT infrastructure by increasingly more sophisticated adversaries both from traditional adversaries, but also from adversaries attempting to profit from intellectual property at the Labs to the Personally Identifiable Information (PII) of DOE personnel.

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 that control access and protect S&S interests, 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. The Protective Force response and deployment configurations at SC laboratories reflect some of the most advanced tactical operator skills within the US government (e.g., the armed security police officers protecting Building 3019 at ORNL), which are necessary due to the inherent consequences of protecting weapons grade nuclear materials, critical program assets, and classified information. 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, 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, sensors, surveillance devices, access control systems, and power systems. In addition, the continued use of AI-based technologies provides further enhance performance with respect to sites' abilities to detect, identify, track, and classify physical security threats, 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 Lawrence Berkeley National 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.

Cybersecurity

The Cybersecurity program element develops and maintains a comprehensive program for ten national laboratories and three dedicated offices. There are numerous advanced persistent threats (APTs) with the goals of disrupting vital DOE SC missions and stealing critical research intellectual property in the areas of Artificial Intelligence, Material Science, High Performance Computing, and Basic Energy Science. The risks from these APTs include not only disrupting the missions of SC and stealing intellectual property, but also acquiring PII of the members of both the Federal and contractor workforce. This program element's goals are to enable mission and science, align cyber funding for risk reduction, strengthen security posture by embracing new security designs, and offer unified guidance and cybersecurity procedures. The Cybersecurity program element responds to cyber incidents by supporting the activities needed for incident management, prosecution, and investigation of cyber intrusions. The program element supports both disaster recovery and incident recovery, as well as notifications within the cybersecurity community. Based on Departmental directives, the SC cybersecurity program management, site initiatives, and IT infrastructure management comprise the final component of the cybersecurity program element.

The increasing costs of cybersecurity tools limit the pace at which SC can reach full adherence to congressional and OMB cyber and IT requirements.

Personnel Security

The Personnel Security program element is critical to identification of predictors of potentially dangerous or destructive behavior and encompasses the 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. The program processes the large number of foreign visitors that engage with the 10 Science laboratories to mitigate Nation State information and intelligence collection efforts.

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. This 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 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. In addition, this program element includes the performance of vulnerability and/or risk assessments, which provide a technical basis for the integrated security program at the site and the acceptance of any associated residual risk.

Safeguards and Security
Funding

(dollars in thousands)

	FY 2024 Enacted	FY 2025 Enacted	FY 2026 Request	FY 2026 Request vs FY 2025 Enacted
Safeguards and Security				
Protective Forces	53,911	57,732	57,908	+176
Security Systems	27,012	21,068	20,227	-841
Information Security	5,830	5,830	5,804	-26
Cybersecurity	82,497	82,497	82,497	–
Personnel Security	9,327	10,553	10,794	+241
Material Control and Accountability	3,054	3,494	3,767	+273
Program Management	8,369	8,826	9,003	+177
Total, Safeguards and Security	**190,000**	**190,000**	**190,000**	**–**

Safeguards and Security
Explanation of Major Changes

(dollars in thousands)

FY 2025 Enacted		FY 2026 Request	Explanation of Changes FY 2026 Request vs FY 2025 Enacted
Safeguards and Security	**$190,000**	**$190,000**	**$—**
Protective Forces	$57,732	$57,908	+$176
Funding continues 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 maintain 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, the Request will support training for these perishable skills, thereby ensuring the readiness of our security officers at all SC laboratories.	Funding will support sustained levels of operations and training at increased overhead, inflation, and contractually obligated Cost of Living Adjustments for Protective Forces.
Security Systems	$21,068	$20,227	-$841
Funding continues 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 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.	Funding will address sustained levels of operations at increased overhead and inflation rates. Additionally, the funding supports the replacement of highest priority end of life security across the 13 SC sites.
Information Security	$5,830	$5,804	-$26
Funding continues 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 the personnel, equipment, training, and systems necessary to ensure the growing SC mission and associated sensitive and classified information is safeguarded at SC laboratories.	Funding will support sustained levels for Information Security activities at increased overhead and inflation rates.

(dollars in thousands)

FY 2025 Enacted	FY 2026 Request	Explanation of Changes FY 2026 Request vs FY 2025 Enacted
Cybersecurity $82,497	$82,497	$ —
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, funding continues the 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 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 Request will continue 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.	Funding will support sustained efforts to continue implementing Executive Order 14028 requirements to include Zero Trust Infrastructure at increased overhead and inflation rates.
Personnel Security $10,553	$10,794	+$241
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 continues to support the processing of the large number of foreign visitors that engage with the 10 Science laboratories, which is vital to thwarting known Nation State information and intelligence collection efforts.	The Request will continue 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, the Request will support the processing of the large number of foreign visitors that engage with the 10 Science laboratories, which is vital to thwarting known Nation State information and intelligence collection efforts.	Funding will provide sustained support for personnel security at increased overhead and inflation rates.

(dollars in thousands)

FY 2025 Enacted	FY 2026 Request	Explanation of Changes FY 2026 Request vs FY 2025 Enacted
Material Control and Accountability $3,494	$3,767	+$273
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 continue 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.	Funding will provide sustained support for MC&A activities at increased overhead and inflation rates.
Program Management $8,826	$9,003	+$177
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 continue to perform as designed through on-going testing and assurance activities.	The Request will continue 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.	Funding will provide sustained support for Program Management activities at increased overhead and inflation rates.