Safeguards and Security

Overview

The SC Safeguards and Security (S&S) program is designed to ensure appropriate security measures are in place to support the SC mission requirements of open scientific research and to protect critical assets within these SC laboratories. Accomplishing this 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 process. Threats to these SC high-consequence assets and capabilities come from an array of evolving sources being followed by the DOE's Office of Intelligence/Counterintelligence, National intelligence agencies and local law enforcement agencies 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. To counter these threats and support operations, the physical security program continually looks to leverage the latest security technologies and tactics, to include artificial intelligence (AI) systems and software to enhance program performance and efficiency in addressing 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.

Highlights of the FY 2025 Request

The FY 2025 Request for S&S is $195.0 million, an increase of $11 million over the FY 2023 Enacted. The FY 2025 Request will prioritize the retention of existing security in the physical security funding allocation. SC will also maintain the current capability of the HSPD-12 credentialing effort focused on high-priority actions to support the screening of the uncleared personnel population have access to the highest risk assets at SC sites (e.g., information technology networks).

The FY 2025 Request includes $83.3 million in Cybersecurity to address long-standing gaps in infrastructure, operations, and compliance to ensure adequate detection, mitigation, and recovery from cyber intrusions and attacks against DOE laboratories. Funding in this Request supports the implementation of Executive Order 14028 requirements for Multi-Factor Authentication (MFA) to the maximum extent possible, 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 such as Russia, China and North Korea, 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 their coordinated efforts with federal and local law enforcement agencies, are our first line of defense against any violent attack against DOE personnel. This includes responding to, reporting, and defending against any number of events, including those resembling the nearly 600 mass shootings in the United States that have occurred since 2020. 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, which are necessitated 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, random 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 interests. The Security Systems program element provides the backbone of the physical protection of Departmental personnel, material, equipment, property, and facilities through the deployment of various systems. 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 enhanced 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.

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 as a result of SC's growth in national security activities and federal requirements to digitize millions of pages of scientific working documents.

Cybersecurity

The Cybersecurity program element develops and maintains a comprehensive program for ten national laboratories and four dedicated offices. There are numerous advanced persistent threats (APTs) from countries such as China, Russia, and North Korea with the goals of disrupting vital DOE SC missions and stealing critical research intellectual property in the areas of 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 DOE directives, the DOE cybersecurity program management, site initiatives, and infrastructure management comprise the final component of the Cybersecurity program element.

Personnel Security

The Personnel Security program element is critical for identifying 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 classified information or material. Additionally, this program element addresses the process of vetting the vast 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, awareness programs for Federal and contractor employees. Lastly, the program also processes the large number of foreign visitors that engage with the ten Science laboratories to thwart known 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 coordinates the management of Protective Forces, Security Systems, Information Security, Personnel Security, and MC&A to achieve and ensure appropriate levels of protections and integration 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 need for acceptance of any associated residual risks.

Safeguards and Security
Funding

(dollars in thousands)

	FY 2023 Enacted	FY 2024 Annualized CR	FY 2025 Request	FY 2025 Request vs FY 2023 Enacted
Safeguards and Security				
Protective Forces	52,341	53,911	54,300	+1,959
Security Systems	24,693	35,812	31,640	+6,947
Information Security	5,660	5,830	5,800	+140
Cybersecurity	81,260	83,697	83,260	+2,000
Personnel Security	9,055	9,327	9,000	-55
Material Control and Accountability	2,965	3,054	3,000	+35
Program Management	8,125	8,369	8,000	-125
Total, Safeguards and Security	**184,099**	**200,000**	**195,000**	**+10,901**

Safeguards and Security
Explanation of Major Changes

(dollars in thousands)

FY 2023 Enacted	FY 2025 Request	Explanation of Changes FY 2025 Request vs FY 2023 Enacted
Safeguards and Security $184,099	**$195,000**	**+$10,901**
Protective Forces $52,341	$54,300	+$1,959
Funding supports security officers and their required equipment and training necessary to maintain proper protection levels 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 $24,693	$31,640	+$6,947
Funding supports security systems in place as well as continued implementation of security modifications that address both the revised DBT and Science and Technology Policy.	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 increases will address sustained levels of operations at increased overhead and inflation rates.

(dollars in thousands)

FY 2023 Enacted	FY 2025 Request	Explanation of Changes FY 2025 Request vs FY 2023 Enacted
Information Security $5,660	$5,800	+$140
Funding supports personnel, equipment, and systems necessary to ensure 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.
Cybersecurity $81,260	$83,260	+$2,000
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 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.

(dollars in thousands)

FY 2023 Enacted	FY 2025 Request	Explanation of Changes FY 2025 Request vs FY 2023 Enacted
Personnel Security $9,055	$9,000	-$55
Funding supports Personnel Security efforts at SC laboratories as well as SC Headquarters security investigations.	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 ten Science laboratories, which is vital to thwarting known Nation State information and intelligence collection efforts.	Funding will provide sustained support for personnel security.
Material Control and Accountability $2,965	$3,000	+$35
Funding supports functions ensuring Departmental materials are properly controlled and accounted for at all times.	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 $8,125	$8,000	-$125
Funding supports oversight, administration, and planning for security programs at SC laboratories and provides integration of all security elements and security procedures protecting SC Research missions.	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.