Safeguards and Security

Overview

The Department of Energy's (DOE) Office of Science (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 SC laboratories. Accomplishing this mission depends on providing physical and cyber controls that will mitigate possible risks to the laboratories' employees, nuclear and special materials, classified and sensitive information, hazardous materials, mission essential functions and facilities. The SC S&S program also provides funding for cybersecurity for the laboratories' information technology systems to protect computers, networks, and data from unauthorized access.

Highlights of the FY 2024 Request

The FY 2024 Request for S&S is $200.0 million. The FY 2024 Request supports sustained levels of operations in S&S program elements including Protective Forces, Security Systems, Information Security, Cybersecurity, Personnel Security, Material Control and Accountability, and Program Management.

The FY 2024 Request includes $83.7 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 Maximum Multi-Factor Authentication (MFA), Maximum Encryption, Cloud Strategy/Security, Improved Logging and Supply Chain Management, and Zero Trust Infrastructure.

The FY 2024 Request supports the S&S program's highest priority, which is to provide adequate security for the protection of Category I quantities of special nuclear material housed in Building 3019 at the Oak Ridge National Laboratory (ORNL).

The FY 2024 Request supports the implementation of key and mandatory National and Departmental security policies. Funding supports the sustainment of security operations at the national laboratories at the asset-level and along the site and building boundaries and security areas. These protections include the sustainment of physical countermeasures that provide deterrence, detection, delay, and response; asset-level accounting and control programs; employee and visitor verification and eligibility programs, and program performance and assurance processes. The funding also supports the continuation of the phased implementation of new standards, such as the standard to conduct background investigations on long-term uncleared personnel with physical and logical access. The funding supports the modernization and/or replacement of select risk and priority-driven security systems infrastructure. These systems mitigate threats to a range of national security interests, to include protection of employees (e.g., active shooter), high-consequence hazardous materials, classified matter, and intellectual property as outlined in the Department's Design Basis Threat (DBT) policy. The FY 2024 Request provides the resources to continue to implement the administration's policies associated with foreign national collaborations that assure the protection of U.S. science and technology. These new security mandates include the review of curriculum vitae to determine what intellectual capital to permit access to and rigorous validation of immigration documentation.

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. 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 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
The Security Systems program element provides the backbone of the physical protection of Departmental personnel, material, equipment, property, and facilities through the deployment of HSPD-12 and local credentials, entry control points, fences, barriers, lighting, sensors, surveillance devices, access control systems, and power systems operated and used to support the protection of people, DOE property, classified information, and other interests of national security.

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.

Cybersecurity
The Cybersecurity program develops and maintains a comprehensive cybersecurity program for ten national laboratories and four dedicated offices. There are numerous adversaries with the goals of disrupting vital DOE SC missions and stealing critical research intellectual property. The cyber goals for the Cybersecurity program are to empower mission and science, align cyber funding to opportunities for risk reduction, strengthen Cybersecurity security posture by embracing new security designs, and offer unified guidance and cybersecurity procedures. The Cybersecurity program responds to cyber incidents by supporting the activities needed to for incident management, prosecution, and investigation of cyber intrusions. The program 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 cybersecurity initiatives, and cybersecurity infrastructure management comprise the final component of the cybersecurity program.

Personnel Security
The Personnel Security program element 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 matter. This element also includes the management of security clearance programs, adjudications, security education, awareness programs for Federal and contractor employees, and processing and hosting approved foreign visitors.

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 element supports administration, including 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 are in place through the conduct of security and/or vulnerability assessments, local threat assessments, and performance assurance activities.

Safeguards and Security
Funding

(dollars in thousands)

	FY 2022 Enacted	FY 2023 Enacted	FY 2024 Request	FY 2024 Request vs FY 2023 Enacted
Safeguards and Security				
Protective Forces	46,710	52,341	53,911	+1,570
Security Systems	22,490	24,693	35,812	+11,119
Information Security	4,490	5,660	5,830	+170
Cybersecurity	81,260	81,260	83,697	+2,437
Personnel Security	5,750	9,055	9,327	+272
Material Control and Accountability	2,500	2,965	3,054	+89
Program Management	6,800	8,125	8,369	+244
Total, Safeguards and Security	**170,000**	**184,099**	**200,000**	**+15,901**

Safeguards and Security
Explanation of Major Changes

(dollars in thousands)

FY 2023 Enacted	FY 2024 Request	Explanation of Changes FY 2024 Request vs FY 2023 Enacted
Safeguards and Security $184,099	**$200,000**	**+$15,901**
Protective Forces $52,341	$53,911	+$1,570
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 training necessary to maintain proper protection levels at all SC laboratories.	Funding will support sustained levels of operations at increased overhead, inflation, and contractually obligated Cost of Living Adjustments for Protective Forces.
Security Systems $24,693	$35,812	+$11,119
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 that address both the revised DBT and Science and Technology Policy.	Funding will support the continued implementation of Homeland Security Presidential Directive 12 (HSPD-12) for uncleared long-term contractor personnel and the associated modernization and replacement of security systems. Funding will support prioritized investments in security infrastructure to provide enhanced protection of assets and to replace end-of-life systems. Funding increases will address sustained levels of operations at increased overhead and inflation rates.
Information Security $5,660	$5,830	+$170
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, and systems necessary to ensure 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 2023 Enacted	FY 2024 Request	Explanation of Changes FY 2024 Request vs FY 2023 Enacted
Cybersecurity $81,260	$83,697	+$2,437
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 (DHS) 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 (DHS) 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 $9,055	$9,327	+$272
Funding supports Personnel Security efforts at SC laboratories as well as SC Headquarters security investigations.	The Request will continue support for Personnel Security efforts at SC laboratories as well as SC Headquarters security investigations.	Funding will provide sustained support for personnel security activities at increased overhead and inflation rates.

(dollars in thousands)

FY 2023 Enacted	FY 2024 Request	Explanation of Changes FY 2024 Request vs FY 2023 Enacted
Material Control and Accountability $2,965	$3,054	+$89
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.	Funding will provide sustained support for MC&A activities at increased overhead and inflation rates.
Program Management $8,125	$8,369	+$244
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, and planning for security programs at SC laboratories and provides integration of all security elements and security procedures protecting SC Research missions.	Funding will provide sustained support for Program Management activities at increased overhead and inflation rates.