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 controls that will mitigate possible risks to the laboratories' employees, nuclear and special materials, classified and sensitive information, 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 2021 Request

The FY 2021 Request for S&S is $115,623,000. The FY 2021 Request supports sustained levels of operations in S&S program elements including Protective Forces, Security Systems, Information Security, Cyber Security, Personnel Security, Material Control and Accountability, and Program Management.

The FY 2021 Request ensures that the S&S program's highest priority is accomplished, which is to provide adequate security for the special nuclear material housed in Building 3019 at the Oak Ridge National Laboratory (ORNL). The Request also ensures the Cyber Security program can adequately detect, mitigate, and recover from cyber intrusions and attacks against DOE laboratories.

The 2018 revision of DOE's Design Basis Threat (DBT) and the then Deputy Secretary's DOE International Science and Technology Engagement Policy (S&T Policy) have shifted DOE's security direction. The DBT addresses protection measures for a more encompassing range of threats and assets than just special nuclear material and classified matter. This revised DBT mandates additional risk assessments and security planning for the protection of chemicals and radioactive sources that could affect persons on-site, whereas, the previous protection standard only addressed quantities that could have an impact off-site. The DBT also calls for "Active Shooter" and "Insider Threat" mitigation. The S&T Policy is designed to protect U.S.-funded research and technologies from sensitive nations who pose high security risks. This includes denying access to restricted areas within DOE laboratories as well as including foreign visitor's Curriculum Vitae (CV) in the Foreign Access Central Tracking System (FACTS).

Implementing both the revised DBT and the S&T Policy is the near- and long-term basis for S&S program and risk mitigating funding decisions at SC laboratories. SC completed implementation planning for the DBT in March 2019 through rigorous Security Risk Assessments and full compliance (based on the most complex laboratories milestones) is expected by September 30, 2022. The S&S program received funding in FY 2020 to begin initial implementation by installing and updating automated access controls to ensure the protection of personnel and intellectual property at SC laboratories. The FY 2021 Request includes an additional $2,923,000 in Security Systems to continue addressing the highest priority items of the DBT and the new S&T Policy.

Description

The S&S program is organized into seven program elements: Protective Forces, Security Systems, Information Security, Cyber Security, Personnel Security, Material Control and Accountability, and 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 DBT and S&T policy implementation through the physical protection of Departmental personnel, material, equipment, property, and facilities, and includes fences, barriers, lighting, sensors,

surveillance devices, entry control 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.

Cyber Security

SC is engaged in protecting the enterprise from a range of cyber threats that can adversely impact mission capabilities. The Cyber Security program element includes central coordination of the strategic and operational aspects of cybersecurity and facilitates cooperative efforts such as the Joint Cybersecurity Coordination Center (JC3) for incident response and the implementation of Department-wide Identity, Credentials, and Access Management (ICAM).

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, Cyber Security, and MC&A to achieve and ensure appropriate levels of protections are in place.

Safeguards and Security
Funding

(dollars in thousands)

	FY 2019 Enacted	FY 2020 Enacted	FY 2021 Request	FY 2021 Request vs FY 2020 Enacted
Protective Forces	43,545	43,545	43,545	—
Security Systems	10,370	16,960	19,883	+2,923
Information Security	4,356	4,356	4,356	—
Cyber Security	33,346	33,346	33,346	—
Personnel Security	5,444	5,444	5,444	—
Material Control and Accountability	2,431	2,431	2,431	—
Program Management	6,618	6,618	6,618	—
Total, Safeguards and Security	**106,110**	**112,700**	**115,623**	**+2,923**

Safeguards and Security
Explanation of Major Changes

(dollars in thousands)

FY 2020 Enacted	FY 2021 Request	Explanation of Changes FY 2021 Request vs FY 2020 Enacted
Safeguards and Security $112,700	**$115,623**	**+$2,923**
Protective Forces $43,545	$43,545	$—
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 provides sustained support for the Protective Forces activity.
Security Systems $16,960	$19,883	+$2,923
Funding supports physical protection of Departmental personnel, material, equipment, property, and facilities, and security infrastructure and systems. Funding also supports initial implementation of security modifications identified in the revised DBT.	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 S&T Policy.	Funding increases to continue implementation of DBT and S&T Policy mandated physical security modifications at SC laboratories. In an effort to address both new initiatives, automated access controls are the program's first priority to protect the workforce and intellectual property and mitigate active shooter and workplace violence threats.
Information Security $4,356	$4,356	$—
Funding supports personnel, equipment, and systems necessary to ensure sensitive and classified information is safeguarded at SC laboratories.	The Request will continue support for the personnel, equipment, and systems necessary to ensure sensitive and classified information is safeguarded at SC laboratories.	Funding provides sustained support for Information Security activities.
Cyber Security $33,346	$33,346	$—
Funding supports protection of laboratory computers, networks, and data from unauthorized access.	The Request will continue support for the protection of laboratory computers, networks, and data from unauthorized access.	Funding provides sustained support for Cybersecurity activities.
Personnel Security $5,444	$5,444	$—
Funding supports Personnel Security efforts at SC laboratories.	The Request will continue support for Personnel Security efforts at SC laboratories as well as SC Headquarters security investigations.	Funding provides sustained support for Personnel Security activities.

(dollars in thousands)

FY 2020 Enacted	FY 2021 Request	Explanation of Changes FY 2021 Request vs FY 2020 Enacted
Materials Control and Accountability $2,431	$2,431	$—
Funding supports functions ensuring Departmental materials are properly controlled and accounted for at all times.	The Request will maintain support for functions ensuring Departmental materials are properly controlled and accounted for at all times.	Funding provides sustained support for MC&A activities.
Program Management $6,618	$6,618	$—
Funding supports oversight, administration, and planning for security programs at SC laboratories and will support security procedures and policy support for SC Research missions.	The Request will maintain support for oversight, administration, and planning for security programs at SC laboratories and will support security procedures and policy support for SC Research missions.	Funding provides sustained support for Program Management activities.

Safeguards and Security
Funding Summary

(dollars in thousands)

	FY 2019 Enacted	FY 2020 Enacted	FY 2021 Request	FY 2021 Request vs FY 2020 Enacted
Other	106,110	112,700	115,623	+2,923
Total, Safeguards and Security	**106,110**	**112,700**	**115,623**	**+2,923**

Safeguards and Security
Estimates of Cost Recovered for Safeguards and Security Activities

In addition to the direct funding received from S&S, sites recover Safeguards and Security costs related to Strategic Partnerships Projects (SPP) activities from SPP customers, including the cost of any unique security needs directly attributable to the customer. Estimates of those costs are shown below.

(dollars in thousands)

	FY 2019 Actual Costs	FY 2020 Planned Costs	FY 2021 Planned Costs
Ames National Laboratory	70	75	70
Argonne National Laboratory	1,000	1,000	1,000
Brookhaven National Laboratory	851	836	835
Lawrence Berkeley National Laboratory	749	751	1,297
Oak Ridge Institute for Science and Education	571	572	577
Oak Ridge National Laboratory	5,163	5,396	5,396
Pacific Northwest National Laboratory	5,500	5,100	5,000
Princeton Plasma Physics Laboratory	55	30	30
SLAC National Accelerator Laboratory	179	190	308
Total, Security Cost Recovered	**14,138**	**13,950**	**14,513**