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 2020 Budget Request

The FY 2020 Request for S&S is $110,623,000. The FY 2020 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 2020 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) 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.

Implementing the revised DBT is the near- and long-term basis for S&S program and risk mitigating funding decisions at SC laboratories. SC is on schedule to complete implementation planning by March 31, 2019, including Security Risk Assessments. Full compliance (based on the most complex laboratories milestones) is expected by September 30, 2022. The S&S program will implement the DBT in stages, starting with the highest priorities including the protection of personnel. The FY 2020 Request includes $4,513,000 to address highest priority items of the DBT.

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, access control officers, and security policy officers assigned to 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 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 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, which supports the Cybersecurity Departmental Crosscut, 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 2018 Enacted	FY 2019 Enacted	FY 2020 Request	FY 2020 Request vs FY 2019 Enacted
Protective Forces	43,545	43,545	43,545	—
Security Systems	10,097	10,370	14,883	+4,513
Information Security	4,356	4,356	4,356	—
Cyber Security	30,619	33,346	33,346	—
Personnel Security	5,334	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	**103,000**	**106,110**	**110,623**	**+4,513**

Activities and Explanation of Changes

FY 2019 Enacted		FY 2020 Request	Explanation of Changes FY 2020 Request vs FY 2019 Enacted
Safeguards and Security	**$106,110,000**	**$110,623,000**	**+$4,513,000**
Protective Forces	$43,545,000	$43,545,000	—
The FY 2019 Enacted budget continues funding to maintain proper protection levels, equipment, and technical training needed to ensure effective performance at all SC laboratories.		The Request will support security officers assigned to protect and respond to S&S interests, along with their related equipment and training.	The FY 2020 Request provides sustained support for the Protective Forces activity.
Security Systems	$10,370,000	$14,883,000	+$4,513,000
The FY 2019 Enacted budget continues funding to maintain the security systems currently in place.		The Request will support 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.	Funding increases to begin implementing DBT mandated physical security modifications at SC laboratories. Automated access controls are the programs first priority to protect the workforce and mitigate active shooter and workplace violence threats.
Information Security	$4,356,000	$4,356,000	$—
The FY 2019 Enacted budget continues funding to maintain personnel, equipment, and systems necessary to ensure sensitive and classified information is safeguarded at SC laboratories.		The Request will support personnel, equipment, and systems necessary to ensure sensitive and classified information is safeguarded at SC laboratories.	FY 2020 funding provides sustained support for Information Security activities.
Cyber Security	$33,346,000	$33,346,000	$—
The FY 2019 Enacted budget continues funding to maintain the necessary level of protection of laboratory computers, networks, and data from unauthorized access.		The Request will support protection of laboratory computers, networks, and data from unauthorized access.	FY 2020 funding provides sustained support for Cybersecurity activities.

FY 2019 Enacted	FY 2020 Request	Explanation of Changes FY 2020 Request vs FY 2019 Enacted
Personnel Security $5,444,000	$5,444,000	$—
The FY 2019 Enacted budget continues funding to maintain Personnel Security efforts at SC laboratories. Funding is requested to support SC Headquarters security investigations.	The Request will support Personnel Security efforts at SC laboratories.	FY 2020 funding provides sustained support for Personnel Security activities.
Materials Control and Accountability $2,431,000	$2,431,000	$—
The FY 2019 Enacted budget continues funding to maintain protection of material at SC laboratories.	The Request will support functions ensuring Departmental materials are properly controlled and accounted for at all times.	FY 2020 funding provides sustained support for MC&A activities.
Program Management $6,618,000	$6,618,000	$—
The FY 2019 Enacted budget continues funding to maintain oversight, administration, and planning for security programs at SC laboratories and supported security procedures and policy support for SC Research missions.	The Request will support oversight, administration, and planning for security programs at SC laboratories and will support security procedures and policy support for SC Research missions.	Program Management funding levels are sustained.

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 2018 Actual Costs	FY 2019 Planned Costs	FY 2020 Planned Costs
Ames National Laboratory	40	70	20
Argonne National Laboratory	1,100	1,000	1,000
Brookhaven National Laboratory	915	851	837
Lawrence Berkeley National Laboratory	1,007	749	1,044
Oak Ridge Institute for Science and Education	509	571	495
Oak Ridge National Laboratory	5,428	5,163	5,163
Pacific Northwest National Laboratory	5,000	5,500	5,500
Princeton Plasma Physics Laboratory	55	55	30
SLAC National Accelerator Laboratory	158	179	190
Total, Security Cost Recovered	**14,212**	**14,138**	**14,279**