Safeguards and Security

Overview

The 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 protecting 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 2019 Budget Request

The FY 2019 Request supports sustained levels of operations in S&S program elements, including Protective Forces, Security Systems, Information Security, Personnel Security, Material Control and Accountability, and Program Management.

The highest priority in the S&S program is to ensure adequate security for the special nuclear material housed in Building 3019 at the Oak Ridge National Laboratory (ORNL).

Another key priority in the FY 2019 Request is to ensure that the Cyber Security element maintains the ability to detect, mitigate, and recover from cyber intrusions and attacks against protected information. In addition, the Request addresses cybersecurity infrastructure necessary to provide security for commensurate investments in IT.

Within the S&S FY 2019 Request, SC supports the Cybersecurity Departmental Crosscut. This includes the Department's CyberOne strategy for managing enterprise-wide cybersecurity and identity authentication for Department of Energy (DOE) IT systems. The CyberOne strategy provides improved Department-wide capabilities for incident management and logical access to federal IT systems.

FY 2019 Crosscuts ($K)

	Cybersecurity
Safeguards and Security	35,332[a]

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 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.

[a] The Cyber Security amount includes $6,435,000 for CyberOne funded through the Working Capital Fund (WCF).

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, provides 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 ($K)

	FY 2017 Enacted	FY 2018 Annualized CR[a]	FY 2019 Request	FY 2019 Request vs FY 2017 Enacted
Protective Forces	39,638	–	41,559	+1,921
Security Systems	10,357	–	10,370	+13
Information Security	4,467	–	4,356	-111
Cyber Security[b]	33,236	–	35,332	+2,096
Personnel Security	6,086	–	5,444	-642
Material Control and Accountability	2,458	–	2,431	-27
Program Management	6,758	–	6,618	-140
Total, Safeguards and Security	**103,000**	**102,301**	**106,110**	**+3,110**

[a] A full-year 2018 appropriation for this account was not enacted at the time the budget was prepared; therefore, the budget assumes this account is operating under the Continuing Appropriations Act, 2018 (Division D of P.L. 115-56, as amended). The amounts included for 2018 reflect the annualized level provided by the continuing resolution. (These amounts are shown only at the Congressional control level and above; below that level, a dash (—) is shown).

[b] The Cyber Security amount includes $6,039,000 in FY 2017 and $6,435,000 in FY 2019 for CyberOne through the Working Capital Fund (WCF).

Safeguards and Security

Activities and Explanation of Changes

FY 2017 Enacted	FY 2019 Request	Explanation of Changes FY 2019 Request vs FY 2017 Enacted
Protective Forces $39,638,000	**$41,559,000**	**+$1,921,000**
Provided funding to maintain proper protection levels, equipment, and technical training needed to ensure effective performance at all SC laboratories.	Continues funding to maintain proper protection levels, equipment, and technical training needed to ensure effective performance at all SC laboratories.	The increase supports protection of the special nuclear material housed in Building 3019 at ORNL, addresses contractual cost of living adjustments, and supports sustained levels of operations across all SC laboratories.
Security Systems $10,357,000	**$10,370,000**	**+$13,000**
Provided funding to maintain the security systems currently in place.	Continues funding to maintain the security systems currently in place.	The increase will ensure proper physical security systems are in place across the SC complex.
Information Security $4,467,000	**$4,356,000**	**-$111,000**
Provided funding to maintain personnel, equipment, and systems necessary to ensure sensitive and classified information is safeguarded at SC laboratories.	Continues funding to maintain personnel, equipment, and systems necessary to ensure sensitive and classified information is safeguarded at SC laboratories.	Information Security decreases to focus efforts on high priority cybersecurity activities.
Cyber Security $33,236,000	**$35,332,000**	**+$2,096,000**
Provided funding to maintain protection of laboratory computers, networks, and data from unauthorized access. This level also continued support of the Department’s CyberOne strategy.	Continues funding to maintain a proper level of protection of laboratory computers, networks, and data from unauthorized access. The Request also continues support of the Department’s CyberOne strategy.	The increase will provide funding to support enhanced Cyber Security protection from cyber intrusions and attacks against protected information. The increase also supports the Department’s CyberOne strategy.
Personnel Security $6,086,000	**$5,444,000**	**-$642,000**
Provided funding to maintain Personnel Security efforts at SC laboratories.	Continues funding to maintain Personnel Security efforts at SC laboratories. Funding is requested to support SC Headquarters security investigations.	Personnel Security decreases to focus efforts on high priority cybersecurity activities. The Request includes additional funding for security investigations that will support the consolidation of Headquarters security investigations and clearances in SC.

FY 2017 Enacted	FY 2019 Request	Explanation of Changes FY 2019 Request vs FY 2017 Enacted
Materials Control and Accountability $2,458,000	**$2,431,000**	**-$27,000**
Provided funding to maintain protection of material at SC laboratories.	Continues funding to maintain protection of material at SC laboratories.	Materials Control and Accountability decreases slightly to focus efforts on high priority cybersecurity activities.
Program Management $6,758,000	**$6,618,000**	**-$140,000**
Provided funding to maintain oversight, administration, and planning for security programs at SC laboratories and supported security procedures and policy support for SC Research missions.	Continues funding to maintain oversight, administration, and planning for security programs at SC laboratories and will support security procedures and policy support for SC Research missions.	Program management decreases to focus efforts on high priority cybersecurity activities.

Estimates of Cost Recovered for Safeguards and Security Activities ($K)

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.

	FY 2017 Planned Costs	FY 2018 Planned Costs	FY 2019 Planned Costs
Ames National Laboratory	40	40	75
Argonne National Laboratory	1,100	1,100	1,500
Brookhaven National Laboratory	1,218	915	911
Lawrence Berkeley National Laboratory	1,010	1,007	966
Oak Ridge Institute for Science and Education	677	509	512
Oak Ridge National Laboratory	4,710	5,428	5,428
Pacific Northwest National Laboratory	4,781	5,000	5,001
Princeton Plasma Physics Laboratory	50	55	55
SLAC National Accelerator Laboratory	135	158	235
Total, Security Cost Recovered	**13,721**	**14,212**	**14,683**