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 requirement of open scientific research and to protect critical assets within SC laboratories. This is accomplished by 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 2018 Budget Request

The FY 2018 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). SC is proactive in evaluating and improving security at that facility and includes funding to do so.

As another key priority, the FY 2018 Request ensures that the Cyber Security element maintains the ability to detect, mitigate, and recover from cyber intrusions and attacks against protected information.

Within the S&S FY 2018 Request, SC supports the Cybersecurity Departmental Crosscut. This includes the Department's CyberOne strategy for managing enterprise-wide cyber security and identity authentication for Department of Energy (DOE) information technology (IT) systems. The CyberOne strategy provides improved Department-wide capabilities for incident management and logical access to federal IT systems.

FY 2018 Crosscuts ($K)

	Cybersecurity
Safeguards and Security	33,619[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 $6,309,000 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

DOE is engaged in two categories of cyber-related activities: protecting the DOE enterprise from a range of cyber threats that can adversely impact mission capabilities and improving cybersecurity in the electric power subsector and the oil and natural gas subsector. The cybersecurity crosscut supports 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 2016 Enacted	FY 2017 Annualized CR[a]	FY 2018 Request	FY 2018 vs FY 2016
Protective Forces	37,899	–	40,545	+2,646
Security Systems	10,097	–	10,097	0
Information Security	7,647	–	4,356	-3,291
Cyber Security[b]	32,974	–	33,619	+645
Personnel Security	5,334	–	5,334	0
Material Control and Accountability	2,431	–	2,431	0
Program Management	6,618	–	6,618	0
Total, Safeguards and Security	**103,000**	**102,805**	**103,000**	0

[a] FY 2017 Annualized CR amounts reflect the P.L. 114-254 continuing resolution level annualized to a full year. 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 $7,093,000 in FY 2016, $4,525,000 in FY 2017, and $6,309,000 in FY 2018 for CyberOne through the Working Capital Fund (WCF). In FY 2016, $1,514,000 was forward funded to address the estimated FY 2017 CyberOne charges of $6,039,000.

Activities and Explanation of Changes

FY 2016 Enacted	FY 2018 Request	Explanation of Changes FY 2018 vs FY 2016
Protective Forces $37,899,000	**$40,545,000**	**+$2,646,000**
Funding provided for this program element maintained protection levels, equipment, and training needed to ensure proper protection and effective performance at all SC laboratories.	Provides funding to maintain proper protection levels, equipment, and technical training needed to ensure effective performance at all SC laboratories.	The increase will ensure adequate 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 at all SC laboratories.
Security Systems $10,097,000	**$10,097,000**	**$0**
Funding provided maintained the security systems in place and supported investments in SC laboratory physical security systems.	Provides funding to maintain the security systems currently in place.	Protection of physical security systems remains at the same level as prior years.
Information Security $7,647,000	**$4,356,000**	**-$3,291,000**
Funding provided for personnel, equipment, and systems necessary to ensure that sensitive and classified information was properly safeguarded at SC laboratories.	Provides funding to maintain personnel, equipment, and systems necessary to ensure sensitive and classified information is safeguarded at SC laboratories.	The decrease reflects the completion of Multi-Factor Authentication implementation for privileged user accounts.
Cyber Security $32,974,000	**$33,619,000**	**+$645,000**
Provided funding to properly protect SC laboratories' computer resources and sensitive data, and to continue support of the Department's CyberOne strategy.	Provides funding to maintain 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 ensure the Cyber Security program element is properly funded to detect, mitigate, and recover from cyber intrusions and attacks against protected information. The increase also supports the Department's CyberOne strategy.
Personnel Security $5,334,000	**$5,334,000**	**$0**
Maintained Personnel Security efforts at SC laboratories.	Provides funding to maintain Personnel Security efforts at SC laboratories.	Personnel Security remains the same level as prior years.
Material Control and Accountability $2,431,000	**$2,431,000**	**$0**
Maintained proper protection of material at SC laboratories.	Provides funding to maintain protection of material at SC laboratories.	Material Control and Accountability remains the same level as prior years.
Program Management $6,618,000	**$6,618,000**	**$0**
Provided funding for oversight, administration, and planning for security programs at SC laboratories and ensured security procedures and policy support for SC research missions.	Provides funding to maintain oversight, administration, and planning for security programs at SC laboratories and will support security procedures and policy support SC Research missions.	Program Management remains the same level as prior years.

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 2016 Current Costs	FY 2017 Planned Costs	FY 2018 Planned Costs
Ames National Laboratory	80	40	40
Argonne National Laboratory	1,100	1,100	1,100
Brookhaven National Laboratory	1,218	1,218	1,218
Lawrence Berkeley National Laboratory	733	1,010	1,007
Oak Ridge Institute for Science and Education	595	677	700
Oak Ridge National Laboratory	4,500	4,710	4,710
Pacific Northwest National Laboratory	5,000	4,781	5,001
Princeton Plasma Physics Laboratory	40	50	55
SLAC National Accelerator Laboratory	120	135	158
Total, Security Cost Recovered	**13,386**	**13,721**	**13,989**