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 electronic data while enabling the SC mission.

Highlights of the FY 2017 Budget Request

Ensuring adequate security for the special nuclear material housed in Building 3019 at the Oak Ridge National Laboratory (ORNL) is the highest priority for the SC S&S Program, and SC is proactive in evaluating and improving security at that facility. The FY 2017 Request includes funding to ensure adequate security at this important facility. The FY 2017 Request supports sustained levels of operations in all S&S functional areas and ensures the Cyber Security program is properly funded to detect, mitigate, and recover from cyber intrusions and attacks against protected information at the heart of the SC mission.

Within the FY 2017 Request, S&S supports the Cyber Security Departmental Crosscut. The Department of Energy (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 Credential and Access Management (ICAM).

FY 2017 Crosscuts ($K)

	Cyber Security
Safeguards and Security	33,236[a]

Finally, the FY 2017 Request continues to support the Department's strategy for managing enterprise-wide cybersecurity and identity authentication for DOE IT systems, referred to as "CyberOne." The CyberOne strategy provides improved Department-wide capabilities for incident management and logical access to federal IT systems.

Description

The S&S program is organized into seven functional areas: Protective Forces, Security Systems, Information Security, Cyber Security, Personnel Security, Material Control and Accountability, and Program Management.

Protective Forces

The Protective Forces 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 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.

[a] Cybersecurity amount includes $6,039,000 for CyberOne funded through the Working Capital Fund (WCF).

Security Systems

The Security Systems 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.

Information Security

The Information Security 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

The Cyber Security element provides appropriate staffing levels, risk management tools, training, and security controls to protect the sensitive and classified data electronically processed, transmitted, or stored on SC IT systems. This element provides site-specific security as well as enterprise-wide security through CyberOne. Risk management controls ensure that IT systems, including the data contained within these systems, maintain confidentiality, integrity, and availability in a manner consistent with the SC mission and federal requirements.

Personnel Security

The Personnel Security 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 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 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 2015 Enacted	FY 2015 Current	FY 2016 Enacted	FY 2017 Request	FY 2017 vs FY 2016
Protective Forces	38,095	37,767	38,805	39,638	+833
Security Systems	12,601	11,314	12,019	10,357	-1,662
Information Security	4,252	4,268	4,416	4,467	+51
Cyber Security[a]	24,118	25,781	33,156	33,236	+80
Personnel Security	5,267	5,335	5,412	6,086	+674
Material Control and Accountability	2,223	2,256	2,454	2,458	+4
Program Management	6,444	6,279	6,738	6,758	+20
Total, Safeguards and Security	**93,000**	**93,000**	**103,000**	**103,000**	**0**

[a] Cybersecurity amount includes $7,351,000 in FY 2015, $6,086,000 in FY 2016, and $6,039,000 in FY 2017 for CyberOne through the Working Capital Fund (WCF).

Safeguards and Security

Activities and Explanation of Changes

FY 2016 Enacted	FY 2017 Request	Explanation of Changes FY 2017 vs FY 2016
Protective Forces $38,805,000	**$39,638,000**	**+$833,000**
Provides funding to maintain protection levels, equipment, and training needed to ensure proper protection and effective performance at all SC laboratories.	The FY 2017 Request will provide funding to maintain proper protection levels, equipment, and technical training needed to ensure effective performance at all SC laboratories.	The increase for protective forces supports sustained levels of operations across all SC laboratories.
Security Systems $12,019,000	**$10,357,000**	**-$1,662,000**
Provides funding to maintain the security systems currently in place and to support investments in SC laboratory physical security systems.	The FY 2017 Request will provide funding to maintain security systems currently in place.	The decrease in security systems is the result of completed prior year investments in laboratory physical security systems.
Information Security $4,416,000	**$4,467,000**	**+$51,000**
Provides funding for personnel, equipment, and systems necessary to ensure sensitive and classified information is properly safeguarded at SC laboratories.	The FY 2017 Request will provide funding for personnel, equipment, and systems necessary to ensure sensitive and classified information is properly safeguarded at SC laboratories.	The increase for information security supports sustained levels of operations across all SC laboratories.
Cyber Security $33,156,000	**$33,236,000**	**+$80,000**
Provides funding to properly protect SC laboratories' computer resources and sensitive data. Funding is also provided to continue support of the Department's CyberOne strategy.	The FY 2017 Request provides funding to ensure the Cyber Security program is properly funded to detect, mitigate, and recover from cyber intrusions and attacks against protected information at the heart of the SC mission. The Request also continues support of the Department's CyberOne strategy.	The increase for cybersecurity supports sustained levels of operations across 12 sites and facilities and continued support for the Departments' CyberOne strategy.
Personnel Security $5,412,000	**$6,086,000**	**+$674,000**
Maintains Personnel Security efforts at SC laboratories.	The FY 2017 Request provides funding for Personnel Security efforts at SC laboratories.	The increase for personnel security supports increased levels of operations across 12 sites and facilities to include credit monitoring and background checks.

FY 2016 Enacted	FY 2017 Request	Explanation of Changes FY 2017 vs FY 2016
Material Control and Accountability $2,454,000	**$2,458,000**	**+$4,000**
Maintains proper protection of material at SC laboratories.	Funding in FY 2017 will provide funding to maintain proper protection of material at SC laboratories.	The increase for material control and accountability supports sustained levels of operations across all SC laboratories.
Program Management $6,738,000	**$6,758,000**	**+$20,000**
Provides funding for oversight, administration, and planning for security programs at SC laboratories and to ensure security procedures and policy support SC research missions.	The FY 2017 Request will provide funding for the oversight, administration, and planning for security programs at SC laboratories and will support security procedures and policy support SC Research missions.	The increase for program management supports sustained levels of operations across all SC laboratories.

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

In addition to the direct funding received from the Safeguards and Security Program, sites recover Safeguards and Security costs related to Work for Others (WFO) activities from WFO customers, including the cost of any unique security needs directly attributable to the customer. Estimates of those costs are shown below.

	FY 2015 Planned Costs	FY 2016 Planned Costs	FY 2017 Planned Costs	FY 2017 vs FY 2016
Ames National Laboratory	80	80	40	-40
Argonne National Laboratory	1,100	1,100	1,100	0
Brookhaven National Laboratory	800	1,218	1,218	0
Lawrence Berkeley National Laboratory	733	733	733	0
Oak Ridge Institute for Science and Education	595	595	677	+82
Oak Ridge National Laboratory	4,500	4,500	4,732	+232
Pacific Northwest National Laboratory	4,633	5,000	5,000	0
Princeton Plasma Physics Laboratory	50	40	50	+10
SLAC National Accelerator Laboratory	76	120	133	+13
Total, Security Cost Recovered	12,567	13,386	13,683	+297