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 cyber security for the laboratories' information technology systems to protect electronic data while enabling the SC mission.

Highlights of the FY 2016 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. Security reviews conducted at Building 3019 since the 2012 security breach at the Y-12 complex have concluded that the materials housed there are properly protected; however, they also highlighted opportunities for improvement, which are currently being implemented. These improvements include clarification of roles and responsibilities, delegation of local Officially Designated Federal Security Authorities, formation of a corrective action team led by a member of SC senior leadership, enhancement of physical security systems, improvement of governance documentation, establishment of a comprehensive S&S Survey Program, and coordination with the DOE Ombudsman to improve the local security culture. The FY 2016 request includes funding to continue providing security at this important facility.

The FY 2016 request also includes an increase in cyber security investments. A review of the SC Cyber Security program was conducted to ensure the full scope of cyber security needs at each laboratory was being captured. The review determined that an increased level of funding was needed. This increase will ensure the Cyber Security Program has the funds needed to defend against cyber security compromises, minimize future losses of protected information, and detect repeated attempts to access information technology assets critical to support the SC mission.

Within the FY 2016 OMB Budget Request, S&S supports the Cyber Security Departmental Crosscut. DOE is engaged in three categories of cyber-related activities: protecting the DOE enterprise from a range of cyber threats that can adversely impact mission capabilities; bolstering the U.S. Government's capabilities to address cyber threats; 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 for incident response and the implementation of Department-wide Identity Credential and Access Management.

FY 2016 Crosscuts ($K)

	Cyber Security	Total
Safeguards and Security	33,156[a]	33,156

[a] Cybersecurity amount includes $6,086,000 for CyberOne through the Working Capital Fund (WCF).

The Department is continuing its strategy for managing enterprise-wide cyber-security 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. SC continues support of this Department-wide investment at the FY 2015 level. DOE's cybersecurity policy establishes line management accountability for ensuring protection of information and information systems through senior DOE management, including the Department's Under Secretaries. Departmental elements will provide sufficient direct funding to (or contractually direct) DOE labs and sites to implement cybersecurity, site-specific incident response capabilities, and the Department's risk management approach.

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.

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, and 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 2014 Enacted	FY 2014 Current	FY 2015 Enacted	FY 2016 Request	FY 2016 vs. FY 2015
Protective Forces	38,502	38,502	38,095	38,805	+710
Security Systems	13,580	13,580	12,601	12,019	-582
Information Security	4,407	4,407	4,252	4,416	+164
Cyber Security	16,074	16,074	24,118[a]	33,156[a]	+9,038
Personnel Security	5,416	5,416	5,267	5,412	+145
Material Control and Accountability	2,522	2,522	2,223	2,454	+231
Program Management	6,499	6,499	6,444	6,738	+294
Total, Safeguards and Security	**87,000**	**87,000**	**93,000**	**103,000**	**+10,000**

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

Activities and Explanation of Changes

FY 2015 Enacted	FY 2016 Request	Explanation of Changes FY 2016 vs. FY 2015
Protective Forces $38,095,000	**$38,805,000**	**+$710,000**
Provides funding to maintain protection levels, equipment, and training needed to ensure proper protection and effective performance at all SC laboratories.	The FY 2016 Request will provide funding to support contracts that must adhere to cost of living adjustments required by collective bargaining agreements and to also maintain proper protection levels, equipment, and technical training needed to ensure effective performance at all SC laboratories.	The increase for protective forces across 12 sites and facilities is indicative of sustained levels of operations.
Security Systems $12,601,000	**$12,019,000**	**-$582,000**
Provides funding to maintain the security systems currently in place and to support investments in SC laboratory physical security systems. .	The FY 2016 Request will provide funding to properly maintain security systems and to support modest investments in upgrades to SC physical security monitoring, detection and access control systems.	The decrease reflects completion of prior year physical security upgrades.
Information Security $4,252,000	**$4,416,000**	**+$164,000**
Provides funding for personnel, equipment, and systems necessary to ensure sensitive and classified information is properly safeguarded at SC laboratories.	The FY 2016 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 the SC-wide information security program across 12 sites and facilities is indicative of sustained levels of operations.

FY 2015 Enacted	FY 2016 Request	Explanation of Changes FY 2016 vs. FY 2015
Cyber Security $24,118,000 Maintains proper protection of SC laboratory computer resources and data and also supports SC's contribution of the Department's CyberOne strategy, which is managed through the Working Capital Fund. CyberOne is the Department's solution for managing enterprise-wide identity management and cyber-security for DOE systems and data. CyberOne will consolidate and streamline Department-wide systems and business processes to mitigate the risk of intrusion and the threat such intrusions pose to high-valued national assets. CyberOne will integrate various tools at headquarters and across the DOE complex to secure both data transmission and data repositories at these diverse sites.	$33,156,000 The FY 2016 request will support proper protection of the SC laboratories' computer resources and sensitive data. A review of the SC Cyber Security program was conducted to ensure the full scope of cyber security needs at each laboratory was being captured. The review determined that, in order to properly protect each SC laboratory from cyber threats, increased funding for the program was needed. In FY 2016, Cyber Security will also continue to support the Department's CyberOne strategy.	+$9,038,000 The increase supports the full scope of Cyber Security tools, licenses, and FTE requirements across 12 sites and facilities.
Personnel Security $5,267,000 Maintains Personnel Security efforts at SC laboratories.	$5,412,000 FY 2016 funding will maintain Personnel Security efforts at SC laboratories.	+$145,000 Funding increases slightly in response to increased requests across all sites for required personnel security investigations and increased visitor control activities at SC sites and facilities.
Material Control and Accountability $2,223,000 Maintains proper protection of material at SC laboratories.	$2,454,000 Funding in FY 2016 will maintain proper protection of material at SC laboratories and supports required staffing levels needed to ensure the sites' baseline levels of MC&A operations can be achieved.	+$231,000 The increase is to accommodate required staffing level needs to ensure proper levels of MC&A operations can be achieved.
Program Management $6,444,000 Provides funding for the oversight, administration, and planning for security programs at SC laboratories and to ensure security procedures and policy support SC Research missions.	$6,738,000 The FY 2016 Request will provide funding for the oversight, administration, and planning for security programs at SC laboratories and to ensure security procedures and policy support SC Research missions.	+$294,000 The increase is indicative of sustained levels of operations.

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 2014 Planned Costs	FY 2015 Enacted Costs	FY 2015 Planned Costs	FY 2016 Planned Costs	FY 2016 vs. FY 2015
Ames National Laboratory	80	80	80	80	0
Argonne National Laboratory	1,470	1,100	1,100	1,100	0
Brookhaven National Laboratory	800	800	800	800	0
Lawrence Berkeley National Laboratory	733	733	733	733	0
Oak Ridge Institute for Science and Education	595	595	595	595	0
Oak Ridge National Laboratory	4,500	4,500	4,500	4,500	0
Pacific Northwest National Laboratory	4,800	4,633	4,633	4,204	-429
Princeton Plasma Physics Laboratory	50	50	50	40	-10
SLAC National Accelerator Laboratory	69	76	76	76	0
Total, Security Cost Recovered	13,097	12,567	12,567	12,128	-439