Safeguards and Security

Funding Profile by Subprogram

(dollars in thousands)

	FY 2010 Current Appropriation	FY 2012 Request
Safeguards and Security		
Protective Forces	35,059	37,147
Security Systems	11,896	10,435
Information Security	4,655	4,595
Cyber Security	16,119	15,042
Personnel Security	5,835[a]	6,905[a]
Material Control and Accountability	2,319	2,379
Program Management	7,117	7,397
Total, Safeguards and Security	83,000	83,900

Public Law Authorizations:

Public Law 95–91, "Department of Energy Organization Act", 1977
Public Law 109–58, "Energy Policy Act of 2005"
Public Law 110–69, "America COMPETES Act of 2007"
Public Law 111–358, "America COMPETES Act of 2010"

Program Overview

Mission

The mission of the Office of Science (SC) Safeguards and Security (S&S) program is to support the Departmental research missions at SC laboratories by ensuring appropriate levels of protection against unauthorized access, theft, or destruction of Department assets, and hostile acts that may cause adverse impacts on fundamental science, national security, and the health and safety of DOE and contractor employees, the public, and the environment.

Background

The S&S program ensures that the SC mission can be conducted in an environment that is secure and free from acts which may cause adverse impacts on the continuity of the program. Because SC laboratories collaborate with universities and research facilities in every corner of the globe, the physical and virtual security posture at SC laboratories must be flexible and supportive of these information exchanges and collaborative efforts. As a result, the S&S program is built on a foundation that enables each facility to design varying degrees of protection commensurate with the risks and consequences for that facility.

[a] For security investigations, FY 2010 includes direct appropriations funding of $184,000 for federal field personnel; an estimated additional $5,816,000 for contractors investigations are funded through chargebacks to the programs requiring the clearances. The corresponding FY 2012 amounts are $272,000 and $5,000,000.

In FY 2010, SC evaluated best practices in security at similar federal and private institutions. Based on that study, SC defined a standard set of security measures, the SC Security Baseline Level of Protection, that provide appropriate protection. The security posture at individual laboratories can be tailored, using the SC Security Baseline Level of Protection as a point of departure, to respond to their individual risks and consequences, while maximizing open collaboration. The end result is an individual security posture at each laboratory, rooted in the SC Security Baseline Level of Protection, that forms the basis for site security operations and funding decisions.

The Security Baseline Level of Protection is being implemented in FY 2011. SC is evaluating each site's security posture by conducting a gap analysis between the current posture and the baseline, and identifying the activities and equipment necessary to implement the security posture appropriate for each laboratory. Execution of FY 2011 and FY 2012 funding, as well as future budget requests, will be based on the outcome of those evaluations.

To accomplish its mission, 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.

- The *Protective Forces* element supports security officers/access control officers and security policy officers assigned to protect S&S interests. Activities within this element include the conduct of access control and security response operations as well as physical protection of the Department's critical assets and SC facilities. In addition, activities to maintain operations are aimed at providing effective response to emergency situations; random prohibited article inspections; security alarm monitoring; the collection and destruction of classified information; and constant testing of the protective force to respond to various event scenarios.
- The *Security Systems* element provides for physical protection of Departmental material, equipment, property, and facilities, including buildings, 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 and other interests of national security.

  This element is responsible for entry and access control to ensure individuals entering and leaving facilities are authorized and do not introduce prohibited articles into or remove DOE property. This includes managing barriers, security storage, and lock programs to restrict, limit, delay, or deny entry.
- The *Information Security* element provides support for execution of the administrative policies and procedures to ensure that sensitive and classified information is accurately and consistently identified, reviewed, marked, and appropriately protected 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.
- The *Cyber Security* element provides appropriate security controls for electronically processed, transmitted, or stored sensitive and classified information. Security controls ensure that information systems, including the information contained within the systems, maintain confidentiality, integrity, and availability in a manner consistent with laboratory missions and possible threats.

- The *Personnel Security* element encompasses the processes for security clearance determinations at each site to ensure that individuals are eligible for access to classified information or matter. This element also includes the management of clearance programs, adjudication, security education and awareness programs for DOE federal and contractor employees, and processing and hosting approved foreign visitors.
- The *Material Control and Accountability (MC&A)* element provides assurance that Departmental materials are properly controlled and accounted for at all times. This element also supports (MC&A) administration, including assessing the levels of protection, control, and accounting required for the types and quantities of materials at each facility; documenting facility plans for materials control and accounting; assigning authorities and responsibilities for MC&A functions; ensuring that facility MC&A personnel are trained and qualified to perform their responsibilities; establishing programs to report occurrences such as material theft, the loss of control or inability to account for materials, or evidence of malevolent acts; conducting performance testing of required program elements; and establishing facility programs to conduct and document internal assessments of their operations and MC&A programs.

  MC&A programs are designed to deter theft and diversion of nuclear material by both outside and inside adversaries. The level of control and accountability is graded based on the consequences of their loss.
- The *Program Management* element coordinates the management of Protective Forces, Security Systems, Information Security, Personnel Security, Cyber Security, and Material Control and Accountability to achieve and ensure appropriate levels of protection.
- SC develops S&S plans to implement S&S requirements, conducts surveys to determine whether the requirements have been implemented, responds to national and local threats, and performs a vulnerability analysis that measures the risk of S&S assets. Program Management also supports participation in the quality panel process, which raises issues from the field to headquarters managers and ensures staff is properly educated with respect to security matters.

Benefits

Global information sharing and open scientific collaboration is required for SC to successfully produce scientific breakthroughs. As a result, campuses and networks have been established to allow the world to exchange and access scientific information. These efforts present security challenges across the national laboratory system. The SC Safeguards and Security program is designed to ensure that appropriate measures are in place to address these challenges.

Program Planning and Management

The S&S program established the following goals and priorities in support of the S&S mission:

- Protect special, source, and other nuclear material, radioactive material, and classified and unclassified controlled information at SC laboratories;
- Provide physical controls to SC national laboratory facilities to mitigate other security risks, including risks to facilities and laboratory employees;
- Provide cyber security controls for SC national laboratory information systems to protect data while enabling the mission; and
- Assure site security programs result in the secure workplace required to facilitate scientific advances.

The program is managed using the proven program management principles and approaches applied to other SC programs. To ensure close integration with laboratory operations, S&S employs a fully collaborative and transparent partnership with site offices and laboratory managers.

Budget Overview

The FY 2012 budget request allows sites to maintain program elements at balanced levels and implement an appropriate security posture at each laboratory. In order to ensure S&S program funds are used to support the DOE mission, laboratories will recover costs for any unique security needs required to support Work for Others customers. An estimate of those costs are shown below.

Estimates of Security Cost Recovered by Science, Safeguards and Security

(dollars in thousands)

	FY 2010 Current Appropriation	FY 2012 Request
Safeguards and Security		
Ames National Laboratory	0	40
Argonne National Laboratory	0	1,440
Brookhaven National Laboratory	0	950
Lawrence Berkeley National Laboratory	0	1,547
Oak Ridge Institute for Science and Education	0	400
Oak Ridge National Laboratory	0	4,734
Pacific Northwest National Laboratory	0	3,249
Princeton Plasma Physics Laboratory	0	35
SLAC National Accelerator Laboratory	0	2,794
Thomas Jefferson National Accelerator Facility	0	50
Total, Security Cost Recovered	**0**	**15,239**

Detailed Justification

(dollars in thousands)

	FY 2010 Current Appropriation	FY 2012 Request
Protective Forces	**35,059**	**37,147**

Funding for Protective Forces provides for protective forces in place at SC laboratories where they are needed. Services provided by these forces include screening people and materials for site/facility entry; patrolling the laboratory in search of unauthorized persons and evidence of crime; and monitoring, assessing, and dispatching a response to investigate alarms and reported events. Protective forces also provide emergency management support for natural disasters, and traffic and crowd control for events.

In FY 2012, funding will be used to maintain the protective forces currently in place at a consistent level of effort and will provide for the salaries and benefits for S&S personnel and the equipment, facilities, and training necessary to ensure effective performance.

(dollars in thousands)

	FY 2010 Current Appropriation	FY 2012 Request
Security Systems	**11,896**	**10,435**

Funding for Security Systems provides for the installation, operation, and maintenance and repair of security systems (e.g., alarms, automated access controls, communications equipment, and explosives detection equipment) at SC laboratories. Funding in this sub-element also provides services to ensure the effectiveness of these systems, including activities like performance testing, intrusion detection and assessment, and access enrollment.

In FY 2012, funding will be used to operate and maintain the systems currently in place, including S&S personnel required to operate and service them. In addition, funding supports the required investments in federal access control systems and upgrades (e.g., badge card readers and access system software and hardware) necessary to address the new Homeland Security Presidential Directive-12 (HSPD-12).

Information Security	**4,655**	**4,595**

Funding for Information Security provides for personnel, equipment and systems necessary to ensure sensitive information (e.g., classified documents, unclassified controlled nuclear information, and personal identity information) is properly safeguarded at SC laboratories. Activities include document and material classification and declassification, document marking and storage, and assessing and reporting security infractions.

In FY 2012, funding will be used to provide for S&S personnel, as well as equipment such as alarm systems and technical security countermeasures.

Cyber Security	**16,119**	**15,042**

Funding for Cyber Security provides for the necessary activities to protect SC laboratory computing resources and data against unauthorized access or modification of information, as well as ensuring data availability. These activities include such items as threat assessments, risk management, configuration management, certification/accreditation, training, and network monitoring. For SC, these activities are implemented by an Information Systems Security Manager, a Certification Agent, and full time Information System Security Officer(s).

Funds requested for FY 2012 represent a reduction from FY 2010 levels. Consistent with agency-wide guidance, SC continues to clarify the delineation between Information Technology functions and cyber security functions. As a result, some functions previously charged to Cyber Security (e.g. Plans of Action and Milestones to address vulnerabilities) have been removed from this request and will instead be funded by SC laboratory overhead. FY 2012 funding permits SC to implement a Cyber Security program that ensures that field sites are providing appropriate Cyber Security levels.

Personnel Security	**5,835**	**6,905**

Funding for Personnel Security provides the necessary laboratory S&S personnel to grant individuals access to classified matter and/or special nuclear material and to allow foreign nationals access to SC facilities, consistent with agency procedures. This element also funds security investigations for federal field personnel and security awareness programs for employees.

Funds requested in FY 2012 will be used to maintain support efforts at all SC laboratories.

(dollars in thousands)

	FY 2010 Current Appropriation	FY 2012 Request
Material Control and Accountability	**2,319**	**2,379**

Funding for Material Control and Accountability provides for establishing, controlling, and tracking inventories of special nuclear material and other accountable nuclear material at SC laboratories.

Activities supported by these funds include measurements, quality assurance, accounting, containment, surveillance, and physical inventory.

Funding requested in FY 2012 will ensure that proper protection of material is sustained.

Program Management	**7,117**	**7,397**

Funding for Program Management provides for the oversight, administration, and planning for security programs at SC laboratories. Planning activities include developing annual operating plans and site S&S plans, conducting vulnerability analyses and performance testing, managing security incident reporting, and conducting surveys and self-assessments.

In FY 2012, funding will be used to maintain direction, oversight, administration, and security program planning.

Total, Safeguards and Security	**83,000**	**83,900**

Explanation of Changes

	FY 2012 vs. FY 2010 Current Approp. ($000)
Protective Forces	
Funding maintains the protective forces currently in place at a consistent level of effort and the equipment, facilities, and training necessary to ensure effective performance.	+2,088
Security Systems	
Funding operates and maintains the systems currently in place, including the S&S personnel required to operate and service the systems. The FY 2012 decrease is due to the one-time infrastructure investments that were funded in FY 2010.	-1,461
Information Security	
Funding will be used to provide for the salaries and benefits for S&S personnel, as well as equipment such as alarm systems and technical security countermeasures.	-60
Cyber Security	
Some functions previously charged to cyber security have been removed from this request and will instead be funded by SC laboratory overhead consistent with agency-wide guidance.	-1,077

	FY 2012 vs. FY 2010 Current Approp. ($000)
Personnel Security	
Funds requested in FY 2012 will be used to maintain support for Personnel Security at all SC laboratories. The increased request is for anticipated increases in access and badging costs.	+1,070
Material Control & Accountability	
Funding requested in FY 2012 will ensure that proper protection of material is sustained.	+60
Program Management	
Funding will be used to maintain direction, oversight and administration, and security program planning.	+280
Total Funding Change, Safeguards and Security	**+900**

Supporting Information

Operating Expenses, Capital Equipment and Construction Summary

(dollars in thousands)

	FY 2010 Current Appropriation	FY 2012 Request
Operating Expenses	81,620	83,900
Capital Equipment	734	0
General Plant Projects	646	0
Total, Safeguards and Security	83,000	83,900