

Safeguards and Security
Funding Profile by Subprogram and Activity

(Dollars in Thousands)

	FY 2011 Current	FY 2012 Enacted	FY 2013 Request
Protective Forces	36,522	35,453	33,750
Security Systems	11,625	9,908	13,685
Information Security	4,775	4,753	4,344
Cyber Security	15,604	16,460	18,422
Personnel Security	5,489	5,059	5,000
Material Control and Accountability	2,327	2,189	2,173
Program Management	7,444	6,751	6,626
Total, Safeguards and Security	83,786	80,573^a	84,000

^a The FY 2012 appropriation is reduced by \$1,427,000 for the Safeguards and Security share of the DOE-wide \$73,300,000 rescission for contractor pay freeze savings. The FY 2013 budget request reflects the FY 2013 impact of the contractor pay freeze.

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”

Overview and Benefits

The Safeguards and Security (S&S) program mission is to support Departmental research 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, or the health and safety of DOE and contractor employees, the public, and the environment.

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 exchange and access of 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. Specifically, the program has established the following priorities: to protect special, source, and other nuclear materials, radioactive material,

and classified and unclassified controlled information at SC laboratories; to provide physical controls to SC national laboratory facilities to mitigate other security risks, including risks to facilities and laboratory employees, to an acceptable level; to provide cyber security controls for SC national laboratory information systems to protect data while enabling the mission; and to assure site security programs result in the secure workplace required to facilitate scientific advances.

The S&S program provides the support necessary to ensure the SC mission can be conducted in an open and collaborative environment that is secure 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 the program to adjust protection levels at each facility in response to changes in risks and consequences for that facility.

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.

Program Planning and Management

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.

SC uses a standardized risk-based approach for protection program planning that provides an information baseline for use in integrating S&S considerations, facilitates management evaluation of program elements, determines appropriate resources, and establishes a cost-benefit basis for analyses and comparison. SC sites assess the threat to mission specific assets and processes and implement baseline security elements to mitigate the resulting risk. The result of these efforts is a resource proposal and a site specific S&S Baseline Level of Protection. This baseline level of protection enables the SC research mission at the laboratories in several ways:

- It relies on national standards and rigorous peer reviews where possible, appropriately aligns risk tolerance and acceptance, and recognizes the diversity in the SC sites.
- It provides for the scalability of requirements, defines clear roles and responsibilities, and aligns

accountability for performance with the appropriate Federal and contractor management.

- It encourages the use of technology where appropriate and incorporates the use of risk assessments to drive decisions on protection elements that may exceed or be below the baseline.

SC began implementation of a Security Baseline Level of Protection in FY 2011, but full implementation will take several years. Execution of FY 2011 and FY 2012 funding is based on the outcome of the risk assessments used as the basis for each site’s level of protection. The outcome of those evaluations is the basis for funding requested in FY 2013 and will be the basis for future budget requests.

Explanation of Funding Changes

Consistent with priorities and assumptions, the increased FY 2013 request supports continued implementation of the Security Baseline Level of Protection while also maintaining support for current activities to ensure security is maintained during transition. The funds also support infrastructure investments in site access control systems and upgrades necessary to address Homeland Security Presidential Directive-12 (HSPD-12) requirements, address near-term cyber security threats, and support program enhancements to diminish the likelihood of successful cyber attacks in the future.

(Dollars in Thousands)

FY 2012 Enacted	FY 2013 Request	FY 2013 vs. FY 2012
35,453	33,750	-1,703

Protective Forces

The request is decreased to accommodate funding allocations in Cyber Security and provide the needed enhancements to support a flexible cyber security program capable of responding to emerging threats at SC Laboratories. Implementation of the SC Security Baseline Level of Protection has permitted site-specific incremental reductions in Protective Forces without increasing risk. Funding at this level maintains security posture at a level that is consistent with laboratory needs and supports the equipment, facilities, and training necessary to ensure effective performance.

Security Systems

The increased request is for the required infrastructure investments in federal access control systems and upgrades necessary to address the Homeland Security Presidential Directive-12 (HSPD-12).

9,908 13,685 +3,777

(Dollars in Thousands)

	FY 2012 Enacted	FY 2013 Request	FY 2013 vs. FY 2012
Information Security	4,753	4,344	-409
<p>The request is decreased to accommodate funding allocations in Cyber Security. Funding at this level will ensure proper document marking, storage, and protection of information.</p>			
Cyber Security	16,460	18,422	+1,962
<p>The increased request provides funding to address cyber security needs made apparent by recent attacks and program enhancements needed to ensure that laboratories are properly protected based on individual threat levels. Funding will be used to support threat assessments, risk management, configuration management, and network management.</p>			
Personnel Security	5,059	5,000	-59
<p>The request is decreased to accommodate funding allocations in Cyber Security. Funding at this level maintains support for Personnel Security at all SC laboratories.</p>			
Material Control and Accountability	2,189	2,173	-16
<p>The request is decreased to accommodate funding allocations in Cyber Security. Funding at this level provides resources to maintain essential security activities.</p>			
Program Management	6,751	6,626	-125
<p>The request is decreased to accommodate funding allocations in Cyber Security. Funding at this level maintains direction, oversight and administration, and security program planning.</p>			
Total, Safeguards and Security	80,573	84,000	+3,427

Protective Forces

Overview

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 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, and performance testing of the protective force response to various event scenarios.

Funding and Activity Schedule

Fiscal Year	Activity	Funding (\$000)
2011 Current	Funding for Protective Forces ensured that security personnel were in place at SC laboratories where they are needed. Services provided by these forces included 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 provided emergency management support for natural disasters, and traffic and crowd control for events.	36,522
2012 Enacted	Funding in FY 2012 maintains the necessary protective forces and the equipment, facilities, and training needed to ensure effective performance.	35,453
2013 Request	Funding requested in FY 2013 decreases to accommodate funding allocations in Cyber Security and provide the needed enhancements to support a flexible cyber security program capable of responding to emerging threats at SC Laboratories. SC Security Baseline Level of Protection implementation has permitted site-specific incremental reductions in Protective Forces without increasing risk. Funding maintains the current security posture at a level that is consistent with SC laboratory needs.	33,750

Security Systems

Overview

The Security Systems element provides 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.

Funding and Activity Schedule

Fiscal Year	Activity	Funding (\$000)
2011 Current	Funding for Security Systems provided for the installation, operation, and maintenance and repair of security systems (e.g., automated access controls, communications equipment, and explosives detection equipment) at SC laboratories. Funding also provided services to ensure the effectiveness of these systems, including performance testing, intrusion detection and assessment, and access enrollment.	11,625
2012 Enacted	Funding in FY 2012 maintains the systems currently in place, including S&S personnel required to operate and service them.	9,908
2013 Request	Funding requested In FY 2013 supports the required investments in federal access control systems and upgrades (e.g., badge card readers and access system software and hardware) necessary to meet HSPD-12 requirements.	13,685

Information Security

Overview

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.

Funding and Activity Schedule

Fiscal Year	Activity	Funding (\$000)
2011 Current	Funding for Information Security provided for personnel, equipment, and systems necessary to ensure sensitive and classified information (e.g., classified documents, unclassified controlled nuclear information, and personal identity information) is properly safeguarded at SC laboratories. Activities included document and material classification and declassification, document marking and storage, and assessing and reporting security infractions.	4,775
2012 Enacted	Funding in FY 2012 maintains the level of efforts necessary to provide for S&S personnel as well as equipment such as alarm systems and technical security countermeasures.	4,753
2013 Request	Funds requested in FY 2013 maintain Information Security efforts to ensure proper document marking, storage, and protection of information. The request is decreased to accommodate funding allocations to Cyber Security.	4,344

Cyber Security

Overview

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 the SC Research mission and possible threats.

Funding and Activity Schedule

Fiscal Year	Activity	Funding (\$000)
2011 Current	Funding for Cyber Security provided 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 included threat assessments, risk management, configuration management, certification/accreditation, training, and network monitoring. These activities are implemented by an Information Systems Security Manager, a Certification Agent, and full time Information System Security Officers.	15,604
2012 Enacted	Funding in FY 2012 provides for activities to protect SC laboratory computer resources and data. Consistent with agency-wide guidance, the requested amount reflects the removal of some functions previously charged to Cyber Security that will instead be funded by SC laboratory overhead.	16,460
2013 Request	The increased funding request in FY 2013 addresses emerging cyber security threats and implements an improved cyber security program that ensures laboratories are providing appropriate levels of protections for site specific risk environments and threat levels. Funding will be used to support threat assessments, risk management, configuration management, and network management.	18,422

Personnel Security

Overview

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 Federal and contractor employees, and processing and hosting approved foreign visitors.

Funding and Activity Schedule

Fiscal Year	Activity	Funding (\$000)
2011 Current	Funding for Personnel Security provided 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 funded security investigations for federal field personnel and security awareness programs for employees.	5,489
2012 Enacted	Funding in FY 2012 maintains support for Personnel Security at all SC laboratories.	5,059
2013 Request	Funds requested in FY 2013 maintain support and Personnel Security efforts at all SC laboratories. The request is decreased to accommodate funding increases in Cyber Security.	5,000

Material Control and Accountability

Overview

The Material Control and Accountability (MC&A) element provides assurance that Departmental materials are properly controlled and accounted for at all times. This element supports administration, including performance testing 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. 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.

Funding and Activity Schedule

Fiscal Year	Activity	Funding (\$000)
2011 Current	Funding for Material Control and Accountability provides for establishing, controlling, and tracking inventories of special and other accountable nuclear material at SC laboratories. Activities supported by these funds include measurements, quality assurance, accounting, containment, surveillance, and physical inventory.	2,327
2012 Enacted	Funding in FY 2012 ensures that proper protection of material is sustained.	2,189
2013 Request	Funding requested in FY 2013 provides resources for essential requirements and does not include new or adjusted requirements. The request is decreased to accommodate funding allocations in Cyber Security.	2,173

Program Management

Overview

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 protections are in place. Program Management also puts mechanisms in place to communicate expectations and assess contractor performance and corrective actions to assure continuous improvement.

Funding and Activity Schedule

Fiscal Year	Activity	Funding (\$000)
2011 Current	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.	7,444
2012 Enacted	Funding in FY 2012 maintains direction, oversight, administration, and security program planning. The request decreases due to priority shifts in other critical security elements.	6,751
2013 Request	Funding requested in FY 2013 maintains efforts to ensure security procedures and policy support the SC research mission. The request is decreased to accommodate funding allocations in Cyber Security.	6,626

Supporting Information

Operating Expenses, Capital Equipment and Construction Summary

(Dollars in Thousands)

	FY 2011 Current	FY 2012 Enacted	FY 2013 Request
Operating Expenses	82,526	80,573	84,000
Capital Equipment	220	0	0
General Plant Projects	1,040	0	0
Total, Safeguards and Security	83,786	80,573	84,000

Estimates of Security Cost Recovered by Science, Safeguards and Security

The FY 2013 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. Estimates of those costs are shown below.

(Dollars in Thousands)

	FY 2011 Current	FY 2012 Enacted	FY 2013 Request
Ames National Laboratory	40	40	140
Argonne National Laboratory	1,044	1,440	1,050
Brookhaven National Laboratory	810	950	1,000
Lawrence Berkeley National Laboratory	870	1,547	670
Oak Ridge Institute for Science and Education	440	400	440
Oak Ridge National Laboratory	4,300	4,734	4,500
Pacific Northwest National Laboratory	2,400	3,249	3,881
Princeton Plasma Physics Laboratory	29	35	30
SLAC National Accelerator Laboratory	70	2,794	68
Total, Security Cost Recovered	10,003	15,189	11,779