Department of Energy
Washington, DC 20585

MEMORANDUM FOR DISTRIBUTION

FROM: MARCUS E. JONES
ASSOCIATE DIRECTOR OF SCIENCE FOR
SAFETY, SECURITY AND INFRASTRUCTURE

SUBJECT: Science (SC) Safeguards & Security (S&S) Program Management Plan

In September 2010, a working group composed of SC Federal and laboratory S&S managers developed the SC S&S Baseline Level of Protection (baseline). Please extend my deep appreciation to your representatives for their insights and contributions that were critical in achieving this significant accomplishment. As you know, the baseline is the starting point from which all SC security programs are developed. It has been integrated (as Appendix C) into the Security Program Management Plan (attached).

Please feel free to contact me or have your staff contact Chris McLaughlin, 301-903-7894, (christopher.mclaughlin@science.doe.gov) with any questions you may have.

I look forward to working with you in implementing this mission-enabling process.

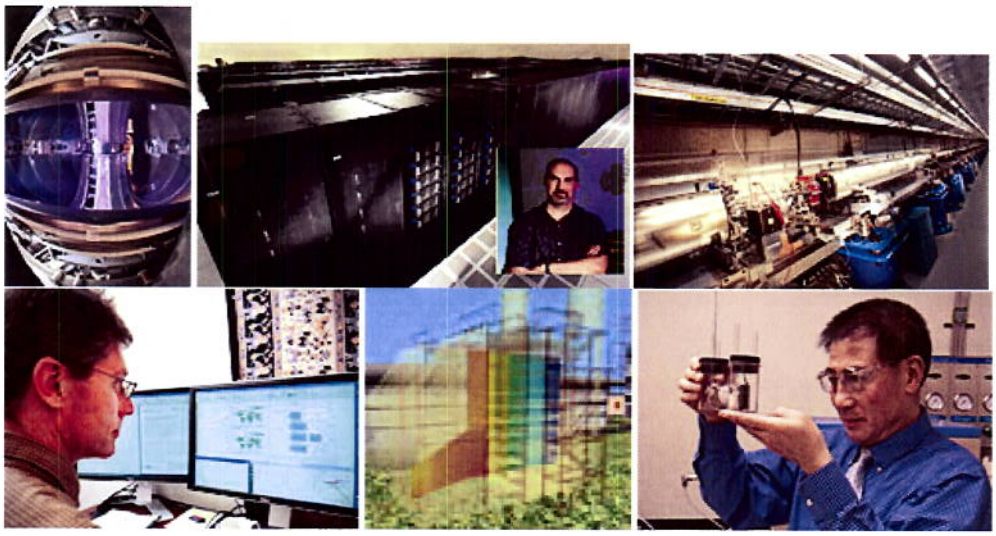
Attachment

cc w/attachment:
G. Malosh, SC-3
J. McBrearty, SC-3
A. Hudak, SC-31
C. McLaughlin, SC-31.3
K. Klausing, SC-41

Distribution List:
Cynthia K. Baebler, Manager, Ames Site Office
Joanna Livengood, Manager, Argonne Site Office
Aundra Richards, Manager, Berkeley Site Office
Michael D. Holland, Manager, Brookhaven Site Office
Roxanne Purucker, Manager, Chicago Office
Michael Weis, Manager, Fermi Site Office
Paul M. Golan, Acting Manager, Oak Ridge Operations Office
Johnny Moore, Manager, Oak Ridge Site Office
Julie Erickson, Acting Manager, Pacific Northwest Site Office
Stephanie Short, Acting Manager, Princeton Site Office
Paul M. Golan, Manager, SLAC Site Office
Joseph Arango, Manager, Thomas Jefferson Site
Walter Warnick, Manager, OSTI

Office of Science
Security Program Management Plan

U.S. DEPARTMENT OF
ENERGY



Issued by:

Associate Director of Science for
Safety, Security and Infrastructure

May 2011

Approved by:

Marcus E. Jones
Associate Director of Science for
Safety, Security and Infrastructure

5/11/2011
Date

Table of Contents

List of Figures

Revision Log

Revision Number	Date	Change Description
0	May 2011	Initial issue

1.0 Purpose

The purpose of the Office of Science (SC) Safeguards and Security (S&S) Program Management Plan is to document the Office of Safety, Security and Infrastructure (SSI) strategy for its management responsibilities with regard to the planning and execution of the SC S&S program. SSI management responsibilities for the SC S&S program include the formulation, advocacy, and execution of the program budget. In executing these responsibilities, SSI relies upon proven management principles and close collaboration with the Site Offices and the Integrated Support Center (ISC) to provide the S&S programmatic direction and decisions necessary to facilitate accomplishment of the mission.

2.0 Office of Science Security Program Mission and Goals

The SC mission is the delivery of scientific discoveries and major scientific tools to transform our understanding of nature and to advance the energy, economic, and national security of the United States. This mission is accomplished through several interconnected goals and objectives: supporting world-leading programs in the science of discovery; advancing national science agendas in the areas of clean energy; understanding the Earth's climate, and supporting the Department's national security missions; and providing national scientific user facilities that serve as the world's 21st Century tools of science. A significant element utilized in accomplishing these objectives is the operation of 10 national laboratories.

In support of the SC mission, the S&S program should ensure appropriate levels of protection against unauthorized access, theft, diversion, loss of custody, destruction of Department assets, or hostile acts that may cause adverse impacts on fundamental science, national security, the health and safety of the Department of Energy (DOE) and contractor employees, the public, and the environment. In order to provide this support, the SC S&S program has established the following goals and priorities:

- Protect special, source, and other nuclear materials, 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, to an acceptable level;
- 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.

Successfully executing the SC mission and goals requires national and international information sharing and open scientific collaboration. The SC S&S program is designed to ensure that appropriate measures are in place given the breadth of mission requirements and assets within SC laboratories. The SC laboratories have many collaborators within and outside the United States. Collaborations occur at the laboratories and remotely through virtual interconnections with universities and research facilities at every corner of the globe. Therefore, the SC physical and cyber security posture must promote integrated international research.

3.0 Approach

The full alignment of the complex-wide SC security program with the Security Program Management Plan will be a multi-year process; therefore, the plan should be an enduring document that allows for a maturing process. As the program office for SC security, SSI is responsible for the programmatic direction and decisions necessary to facilitate mission success. This program is accomplished by providing the following:

- Program objectives that are consistent with SC goals and are sustainable under current and future budget requirements;
- Collaborative relationships with the site offices and the ISC in implementing a program management process that is integrated with the mission and transparent to stakeholders; and
- Streamlined budget formulation and execution processes that minimize the burden on the sites while providing sufficient information to advocate for security program resources and maintain the flexibility to allocate resources.

While there are many outside influences that could affect the DOE security program, the Security Program Management Plan is designed to be an enduring document that sets a course for the SC security program formulation, advocacy, and execution.

SC S&S Program Reform – Beginning in FY 2008, the SC S&S Program undertook an effort to better document the security posture of SC laboratories and to better integrate security with the SC mission. This review was conducted by SSI, the ISC, site offices and laboratory security specialists. The review resulted in a detailed requirements analysis for each laboratory and the ISC development of a Site Security Plan (SSP) template that is used by each of the 10 laboratories to develop and revise their security plans. Subsequently, an independent benchmarking study was conducted comparing SC laboratory security to security at research institutions operated by other federal agencies and the private sector. The result of these efforts is the SC S&S Baseline Level of Protection and program management approach documented in this Security Program Management Plan.

SC Security Baseline Level of Protection – The Department's S&S directives are focused primarily on the need to protect classified information and special nuclear materials. Only four of the SC laboratories (Oak Ridge National Laboratory, Argonne National Laboratory, Brookhaven National Laboratory, and Pacific Northwest National Laboratory) use these materials to a level that requires the DOE Acquisition Regulation security clause be incorporated in their contracts. Only one facility secures Category I Special Nuclear Materials under the DOE Graded Safeguards Policy, and it is classified as a non-enduring facility. Beginning with the formulation of the FY 2013 SC S&S budget, the SC S&S program will include the security baseline indicated by the benchmarking analysis of best practices found in research institutions operated by DOE, other agencies, and the private sector. The baseline guides the development of the site-specific security posture of each of the SC laboratories. This baseline level of protection provides a common starting point for SC in ensuring adequate physical controls and other DOE prescribed security elements are in place at our facilities.

Use of Transparent Budget Planning, Formulation, and Execution Processes – The Site Office Managers (SOMs), ISC, and SSI will implement the Security Program Management Plan through a transparent, collaborative process. The process includes the initial development of a site conceptual baseline (i.e., a high-level summary document which identifies the expected end state site security posture). This process is described in more detail in Section 6.0, and will be based on a collaborative effort among SSI, the site offices, and the ISC.

Security Program Management Plan Assumptions – The following assumptions have been made in formulating this plan:

- The Baseline Level of Protection for SC S&S will provide the flexibility necessary to address the breadth of security needed at all 10 SC laboratories;
- The operations will continue to be direct funded for SC S&S;
- Operations funding will be in compliance with SC S&S uniformly-applied budget and reporting code definitions;
- More than one year may be required to accomplish the site-specific security posture endpoint at all laboratories;
- Capital line item construction projects will include scope and costs for security systems or security-related modifications that are needed;
- If other DOE programs have a need for S&S activities to support their operations beyond what is already provided by the site security program, the site will request necessary funding from that program;
- Beginning in FY 2011, the costs of routine security for Work for Others (WFO) will be provided via full cost recovery. The overhead assessment representing routine security costs for non-DOE sponsors will be phased in during FY 2011 and fully applied beginning in FY 2012. Security requirements driven by specific WFO projects will be directly charged to those customers;
- The S&S program can be successfully executed when DOE and the laboratory contractor are operating through a collaborative relationship; and
- This Security Program Management Plan will be incorporated into the Science Management System (SCMS). Other revisions may also be made to SCMS elements to reflect agreements in the Security Program Management Plan.

4.0 Program Management

The SC S&S program budget is managed by SSI on behalf of the Deputy Director for Field Operations (DDFO) (see Figure 1). The program is managed using the proven program management principles and approaches applied to other SC programs. In addition, because it requires close integration with laboratory operations, it should reflect a fully collaborative and transparent partnership.

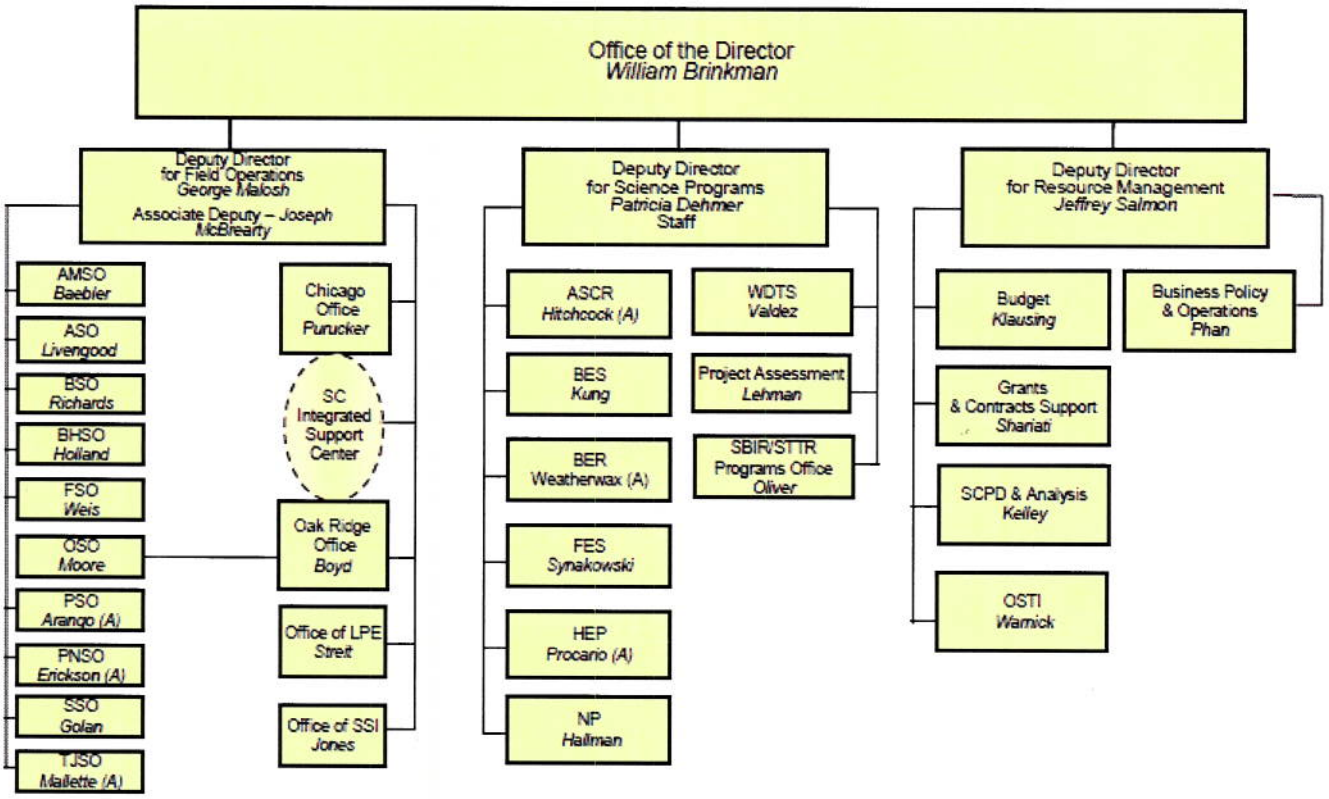


Figure 1. SC Organization

Roles and Responsibilities

An organization chart depicting roles and responsibilities for the SC S&S Program is shown in Figure 2.

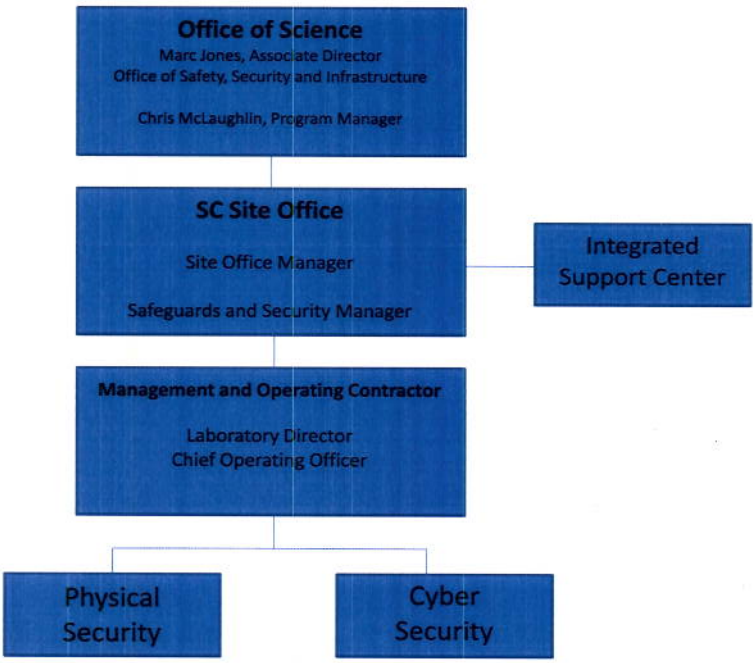


Figure 2. S&S Program Management Structure

SSI Associate Director (AD) – The SSI AD has overall responsibility for the strategic direction, advocacy, and budgeting for the SC S&S program. The AD executes these responsibilities through the Security Program Management Plan in close collaboration with the SC programs, the ISC, and SOMs. The SSI AD works with site office and ISC managers, as needed, to communicate and appropriately address risk.

Security Program Manager – On behalf of the S&S Division Director, a security program manager in the S&S Division has been assigned for the SC Security Program and has been given the following roles and responsibilities:

- Oversee development of program scope and budget, in collaboration with the ISC and site offices;
- Prepare the program budget with support from the field and SC Headquarters organizations;
- Review and provide recommendations to proposed changes for which the SSI AD has approval (see Section 5.0);
- Function as the primary point of contact at DOE Headquarters for S&S program budget matters to all parties external to SC;
- Monitor and evaluate S&S program status during execution through periodic communications; and
- Coordinate Office of Health, Safety and Security (HSS) site assistance review activities when requested by the ISC or SOM.

SOMs – The SOMs are responsible for the administration of the Management and Operating contracts at SC laboratories, which include providing day-to-day direction and oversight of S&S activities at that laboratory. Accordingly, execution of the individual S&S activities at each site is the responsibility of the assigned Site Office staff, with S&S management and technical support from the ISC. Specifically, SOMs' responsibilities include:

- Approval of the Site Security Plan as the Cognizant Security Authority (CSA) to assure the safety and protection of Federal and contractor employees, the environment, and the public at SC's national laboratory sites;
- Routine communication with the SC Director, DDFO, and SSI on S&S matters and performance, and development and implementation of corrective actions;
- Evaluation of S&S performance under his/her respective management and operating contracts; and
- Working with program managers to assure that capital projects include sufficient funding to address security requirements.

ISC – The ISC supports SC SOMs by providing S&S services for sites without security professionals on staff, oversight support through surveys, technical subject matter expertise in S&S issues, and other matters. This includes, but is not limited to, responsibility for determining eligibility for access to

classified matter and/or special nuclear material and implementing the Human Reliability Program for Federal and contractor employees at SC national laboratory sites.

Interfaces with Other SC and DOE Offices

SC Office of Laboratory Policy and Evaluation (OLPE) – OLPE is responsible for the annual laboratory planning process and the SC annual laboratory performance evaluation process. SSI works closely with OLPE and in concert with the SC SOMs to develop guidance and provide feedback for the annual planning and evaluation processes as they relate to the security of SC operations.

SC Science Program Offices (SC-2) – In order to ensure that the security baselines are consistent with long-term SC program goals, SSI will communicate the Security Program Management Plan with SC-2 program offices. It is also anticipated that at sites where funding is dominated by a particular SC program office (Thomas Jefferson National Accelerator Facility, Fermi National Accelerator Laboratory, Princeton Plasma Physics Laboratory, and Ames Laboratory) the SOMs will work closely with the respective program AD to ensure alignment of the site security posture with program strategic goals for laboratory operations. SOMs will also work with program ADs to ensure that capital projects include sufficient funding to address security requirements.

HSS – HSS will be asked for their technical review of the Security Program Management Plan and SC baseline to assure compatibility with DOE policy and oversight. At the request of SOMs, HSS may be asked to provide technical assistance to site offices in their line management role with regard to S&S.

Office of Chief Information Officer (OCIO) – The OCIO is responsible for development of the Department's cyber security governance model in collaboration with the DOE programs. SSI represents the Under Secretary for Science on working groups and committees established by the OCIO to develop and execute the Department's cyber security governance, and to ensure the elements of the Security Program Management Plan relevant to cyber security program budget are directly aligned with the overall Department's cyber security program.

Office of Intelligence and Counterintelligence (IN) – IN has offered to help SC manage intelligence risks in an effective and efficient manner. SC site management, supervisors, and employees will work together with IN to establish a layered insider threat detection and risk assessment program. Each site will work with IN to identify SC intellectual property that needs to be protected from unauthorized disclosure. Senior Counterintelligence Officers (SCIOs) at SC sites will cooperate with SC to generate a tailored threat assessment identifying counterintelligence threats to SC. SCIOs and SC management will then jointly manage risks to SC's valuable intellectual property.

5.0 Planning Baseline Level of Protection Development and Change Control

The SC Security Baseline Level of Protection (Appendix C) is the degree of security provided by the set of countermeasures identified for each facility that must be implemented unless a deviation (up or down) is justified by a risk assessment. It guides the development of the site specific security posture for each SC laboratory. The site-specific security posture is summarized in a conceptual baseline document which identifies the level of site security required to support the site mission and the level of security indicated by the SC security baseline. The posture addresses site factors that influence tailoring the security program to levels at, greater than, or less than those in the SC security baseline. Approval of the conceptual baseline represents an agreement between the SOM and SSI AD on the resources necessary to establish and sustain the proposed site security posture and is therefore jointly signed by the

SOM and SSI AD. Anticipating that the conceptual baseline may take more than one year to fully implement, it will serve as the principle controlling set of priorities for the site's annual budget formulation. The SOM assures that laboratories revise SSPs based on any resulting changes to the site security posture. Though SSPs remain the primary documentation of site security programs and associated risk assessments, sites will not be required to include the SSP in their budget submission.

6.0 Annual Security Budget Formulation and Execution

Budget formulation begins upon receipt of the out-year funding targets provided to SC in the prior year Office of Management and Budget (OMB) pass-back. Funding targets will be provided to SC site offices in an initial budget proposal call issued by SSI (typically in late December/early January). SC laboratory contractors will prepare initial budget proposals consistent with specific funding projections addressed in the OMB pass-back (i.e., over target requests should be included, but must be identified as such).

The initial budget proposal call will establish submission deadlines and request contractor proposals to be delivered to the Site Office, and hence to the SSI program manager, in the form of S&S Budget Information Worksheets for each program element. These budget sheets (which have replaced the requirement for Field Work Proposals) will document funding requested for sub-element level activities and their basis of estimate, along with technical objectives and key assumptions. In addition, the budget sheets will include an integrated priority list for activities requested above the assigned target level. Because Field Work Proposals are no longer required, this approach streamlines the process to minimize the burden on sites and provides information necessary to advocate for and allocate needed resources.

Following submittal of the budget worksheets, the laboratory contractor and SOM will review the budget proposals with SSI via video-teleconference. Subsequently, the SSI AD and SOM will collaborate on developing the budget request to go forward for internal review by the DDFO and Director of Science. SSI will keep the site offices apprised as the budget process moves through the internal phase (late spring/early summer), the OMB submittal (September), and finally the submission of the President's Budget request to Congress the following February. Upon passage of an Appropriation, SSI will coordinate with the SC Office of Budget to issue an Initial Approved Funding Program (AFP) that is consistent with the President's Submission and signed Appropriation. During execution, SOMs may approve shifts in funding among S&S elements to address emerging needs.

7.0 Performance Evaluation and Oversight

SC requires effective CAS at each of its laboratories. Effective systems provide reasonable assurance that the contractor and their parent are meeting expectations of the contract with DOE. DOE through the site office executes contract management, oversight, and contractor performance evaluation. The overall performance of the laboratory in the area of safeguards and security is a specific element of the annual laboratory performance process. The line management responsibility falls primarily on the SOM with subject matter expert support from the ISC, SSI, and HSS when requested. With regard to the S&S program goals and priorities, the S&S program manager will also remain cognizant of the status of progress compared to the site baseline, and the primary objectives of the execution of the S&S budget.

APPENDIX A

Site Specific Conceptual Baseline

FY 2013 Site Specific Conceptual Baseline

Laboratory:	
Prepared By:	**Date:**
Approvals **SOM:** _____ **SSI-AD** _____	

Description:

APPENDIX B

Budget Information Worksheets

Site Element Breakdown Table

Laboratory:

(dollars in thousands)

	FY 2013 Initial Target Provided from Program Office	FY 2013 Site Budget Proposal (Target Level)	FY 2013 Site Budget Proposal (Above Target)
Protective Forces		-	-
Security Systems		-	-
Information Security		-	-
Cyber Security		-	-
Personnel Security		-	-
Material Control & Accountability		-	-
Program Management		-	-
Program Total	-	-	-

Insert Initial FY 2013 Target provided by the budget call.

Enter element totals from the individual Budget Information Worksheets here. Sites may adjust resource levels between elements but the Program Total above should match target provided from program office.

Above Target totals from individual Budget Information Worksheets should be entered here.

FY 2013 Budget Information Sheet

Laboratory:	**S&S Element: Protective Force (Response Capability)**
Prepared by:	**Date:**
Brief Task Description: Includes all personnel and operating costs associated with Protective Forces. This includes such things as salaries, overtime, benefits, travel, materials and supplies, uniforms, equipment, facilities, vehicles, training, communications, Federal and contractor management, and oversight of protective forces.	
This element includes transition plan activities: [ ]Yes [ ]No	

A. Budget:

Sub-element	**Budget ($000)**		**Basis of Estimate**
	Target	**Over Target**	
Salaries, Wages, and Benefits			
Materials and Supplies			
Equipment and Facilities			
Protective Force Training			
Management			
Total FTEs:			
Total			

B. Technical Objective:
This S&S element will meet the following objectives in FY 2013.

C. Key Assumptions used in developing the scope and estimate (including acquisition plan):

D. Deliverables/Schedule:

FY 2013 Budget Information Sheet

Laboratory:	**S&S Element: Security Systems**
Prepared by:	**Date:**
Brief Task Description: Includes all personnel and operating costs associated with designing, installing, performance testing, contraband detection, alarm communications and control, intrusion detection and assessment, barriers and access denial, secure storage, access control, and vital components tampering and monitoring.	
This element includes transition plan activities: [ ]Yes [ ]No	

A. Budget:

Sub-element	**Budget ($000)**		**Basis of Estimate**
	Target	**Over Target**	
Intrusion Detection and Assessment Systems			
Testing			
Access Controls			
Barriers and Delay Mechanisms			
Total FTEs:			
Total			

B. Technical Objective:
This S&S element will meet the following objectives in FY 2013.

C. Key Assumptions used in developing the scope and estimate (including acquisition plan):

D. Deliverables/Schedule:

FY 2013 Budget Information Sheet

Laboratory:	**S&S Element: Information Security**
Prepared by:	**Date:**
Brief Task Description: Includes all personnel salaries, overtime, benefits, and operations and equipment expenses associated with classified documents and materials, classification and declassification, unclassified controlled nuclear information, security infractions, and information protection.	
This element includes transition plan activities: [ ]Yes [ ]No	

A. Budget:

Sub-element	**Budget ($000)**		**Basis of Estimate**
	Target	**Over Target**	
Classified and Controlled Information			
Technical Surveillance Countermeasures			
Operations Security			
Classified Matter Protection and Control			
Total FTEs:			
Total			

B. Technical Objective:
This S&S element will meet the following objectives in FY 2013.

C. Key Assumptions used in developing the scope and estimate (including acquisition plan):

D. Deliverables/Schedule:

FY 2013 Budget Information Sheet

Laboratory:	**S&S Element: Cyber Security**
Prepared by:	**Date:**
Brief Task Description: Includes salaries, overtime, and benefits for an Information Systems Security manager, a Certification Agent, a full time Information Systems Security Officer(s), and SC HQ mandated security improvements. Includes at a minimum, for classified and unclassified data, the management of information technology cyber security assets, cyber information systems, threat assessments, performance measures, risk management, configuration management, certification/accreditation, and training and network monitoring. Cyber related activities that are embedded in normal business operations and Plans of Action and Milestones are excluded.	
This element includes transition plan activities: [ ]Yes [ ]No	

A. Budget:

Sub-element	**Budget ($000)**		**Basis of Estimate**
	Target	**Over Target**	
Information Systems Security Manager			
Information Systems Security Officer(s)			
Certification Agent			
Total FTEs:			
Total			

B. Technical Objective:
This S&S element will meet the following objectives in FY 2013.

C. Key Assumptions used in developing the scope and estimate (including acquisition plan):

D. Deliverables/Schedule:

FY 2013 Budget Information Sheet

Laboratory:	**S&S Element: Personnel Security**
Prepared by:	**Date:**
Brief Task Description: Includes security clearance investigations, adjudication, security education, personnel security assurance program, visitor control, national agency checks, and administrative review activities. Security clearance investigations including initial investigations and reinvestigations may be embedded in the contractor cost of doing business. Contractors will fund contractor personnel investigations where a unique benefiting cost objective cannot be identified. Includes all estimates for processing clearances, adjudication, security awareness and education, visit control, Personnel Security Assurance Program, psychological/medical assessments, foreign visits and assignments and administrative review costs.	
This element includes transition plan activities: [ ]Yes [ ]No	

A. Budget:

Sub-element	**Budget ($000)**		**Basis of Estimate**
	Target	**Over Target**	
Access Authorizations			
Human Reliability Program			
Safeguards and Security Awareness			
Control of Classified Visits			
Unclassified Visits and Assignments by Foreign Nationals			
Total FTEs:			
Total			

B. Technical Objective:
This S&S element will meet the following objectives in FY 2013.

C. Key Assumptions used in developing the scope and estimate (including acquisition plan):

D. Deliverables/Schedule:

FY 2013 Budget Information Sheet

Laboratory:	**S&S Element: Material Control and Accountability**
Prepared by:	**Date:**
Brief Task Description: Includes all personnel and operating and maintenance costs associated with control and accountability of special nuclear materials. Includes salaries, overtime, and benefits for MC&A access areas, surveillance, containment, detection, assessment, testing, transfers, verifications and measurements, inventories, reconciliation, and statistical analysis.	
This element includes transition plan activities: [ ]Yes [ ]No	

A. Budget:

Sub-element	**Budget ($000)**		**Basis of Estimate**
	Target	**Over Target**	
Program Management			
Special Nuclear Material Control			
Special Nuclear Material Accounting			
Special Nuclear Material Measurements			
Physical Inventory			
Total FTEs:			
Total			

B. Technical Objective:
This S&S element will meet the following objectives in FY 2013.

C. Key Assumptions used in developing the scope and estimate (including acquisition plan):

D. Deliverables/Schedule:

FY 2013 Budget Information Sheet

Laboratory:	**S&S Element: Program Management**
Prepared by:	**Date:**
Brief Task Description: Includes all operating and maintenance estimates for planning, professional development and training, inspections, self-assessments, resource planning and implementation for S&S, management and administration, responses to management requests, operations security, technical surveillance countermeasures and facility approval including foreign ownership, control, or influence.	
This element includes transition plan activities: [ ]Yes [ ]No	

A. Budget:

Sub-element	**Budget ($000)**		**Basis of Estimate**
	Target	**Over Target**	
Protection Program Management			
S&S Planning and Procedures			
Management Control			
Program Wide Support			
Total FTEs:			
Total			

B. Technical Objective:
This S&S element will meet the following objectives in FY 2013.

C. Key Assumptions used in developing the scope and estimate (including acquisition plan):

D. Deliverables/Schedule:

FY 2013 Summary of Above Target Priority List

Laboratory:	Prepared by:
Cognizant Security Authority Concurrence:	Date:

S&S Element and Scope	Budget ($000)	Risks if not Funded (Assessment)
		(Submissions are not limited to the space afforded by this summary form. Additional documentation may be provided at the discretion of the site)
Total		

APPENDIX C

Office of Science Safeguards & Security Baseline Level of Protection

Office of Science S&S Baseline Level of Protection

In order to effectively and efficiently protect Departmental assets in a consistent manner, an actionable SC baseline level of protection has been developed. This baseline level of protection:

- Focuses on/enables the laboratories' missions;
- Relies on National Standards and rigorous peer reviews where possible;
- Appropriately aligns risk tolerance and acceptance;
- Recognizes the diversity in the SC sites and provides for the "right size/scalability" of requirements;
- Defines clear roles and responsibilities;
- Aligns accountability for performance with the appropriate Federal and contractor management;
- Encourages the use of technology where appropriate; and
- Incorporates the use of risk assessments/threat analysis to drive decisions on protection elements that may exceed or be below the baseline.

Protection Planning: SC laboratories generally are campus-like environments with few of the assets, such as classified matter and Category I and II Special Nuclear Material (SNM), whose enhanced protection is mandated by law, regulation, and DOE safeguards and security policy. This protection baseline is intended to provide a common basis for SC laboratory security planning and implementation. When a laboratory has assets, such as high value property, critical facilities, classified matter, and/or SNM for which additional protection is required by DOE directives, this protection will take the form of security islands superimposed upon the SC protection baseline.

SC requires implementation of a standardized 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 comparisons. This appendix addresses the SC baseline for physical security and protective forces. This appendix establishes the baseline that is derived from and consistent with DOE security guidance from which site missions and assets may require deviations up or down. Nothing in the SC baseline may be construed as authority to deviate from DOE and SC guidance for security and oversight requirements without approved risk assessments.

Protection Strategies: These are delineated through the Department of Energy (DOE) Manuals and Orders. Individual S&S programs address site-specific characteristics. Strategies applicable to Security Protection Level (SPL) 4 facilities are summarized below:

- Prevent, detect, or deter unauthorized access, modification, or loss of classified and unclassified controlled matter and its unauthorized removal from a site or facility.
- Protect government property (including Category III and IV quantities of nuclear materials) employing a graded approach;
- S&S interests and activities should be protected from theft, diversion, terrorist attack, industrial sabotage, radiological sabotage, chemical sabotage, biological sabotage, espionage, unauthorized access, compromise, and other acts that may have an adverse impact on national security; the environment; or pose significant danger to the health and safety of DOE Federal and contractor employees or the public; and
- Security countermeasures for explosive threats should address a range of activities including hand-carried, mailed, and vehicle-transported devices.

Graded Protection: The Department recognizes that risks must be accepted (i.e., that action cannot be taken to reduce the potential for or consequences of all malevolent events to zero); however, an acceptable level of risk should be determined based on evaluation of a variety of facility-specific goals and considerations. By a graded approach, the department intends that the highest level of protection be given to security interests and activities whose loss, theft, compromise, and/or unauthorized use would seriously affect the national security, the environment, departmental programs, and/or the health and safety of the public or employees. Protection of other interests and activities will be graded accordingly. The approved Graded Security Protection (GSP) and Graded Threat Axis (GTA) will be used as the basis for planning protection programs.

Risk Assessments (RA): Inherent in the open intellectual environment that is recognized to be mission essential for SC are vulnerabilities which adversaries, particularly foreign intelligence adversaries, can exploit with relative ease. These vulnerabilities cannot be completely eliminated without undue damage to the SC mission. Rather, they must be managed in much the same fashion that the financial world manages risks. The RA is used as the base for S&S programs, the results of which are used to design and provide graded protection in accordance with an asset's importance or the impact of its loss, destruction, or misuse.

The DOE's Office of Intelligence and Counterintelligence (IN) has offered to help SC manage intelligence risks in an effective and efficient manner. SC site management, supervisors, and employees will work together with IN to establish a layered insider threat detection and RA program. Each site will work with IN to identify SC intellectual property that needs to be protected from unauthorized disclosure. Senior Counterintelligence Officers (SCIOs) at SC sites will cooperate with SC to generate a tailored threat assessment identifying counterintelligence threats to SC. SCIOs and SC management will then jointly manage risks to SC's valuable intellectual property.

Though the baseline level of protection does not prescribe a mandatory risk assessment method, risk assessments should adhere to recognized principles. These include:

- Provide a credible assessment of the threat, consequences, and vulnerability to specific acts;
- Produce similar or identical results when applied by various professionals; and
- Is defensible and provides sufficient justification for deviation from the baseline.

DOE G 470.4-1, Approved: 8-21-08, *ASSET PROTECTION ANALYSIS GUIDE,* and the Interagency security committee standard for risk assessments both describe acceptable risk assessment processes. The risk assessment process used must be described in the SSP as well as the CSA approved training certification or equivalent experience of the practitioner.

Site Security Plan (SSP): All sites must develop a SSP to describe the protection program in accordance with the SC SSP template. The SSP's should include the results of the risk assessment(s) that document the threat and targets (e.g., theft or sabotage of targets; theft of research sensitive information, or classified matter; or sabotage of research materials, equipment, or results) and the risk associated with the threat. SSPs document the protection strategies and associated areas/elements established to mitigate risk at a site.

A graded approach should be employed that differentiates security elements used to protect facilities and assets. Key information will be included for security managers to make budgetary and risk decisions. The SSP is the overarching standard to which oversight audits, assessments, and

inspections are conducted. The types of assets, processes, and missions that require protection should be described. It should be comprehensive and address other required Federal security requirements, e.g., Mailroom Security and Transportation Security Plans for Nuclear Materials and Hazardous Materials. SSPs must be approved by the local DOE cognizant security authority (CSA). The SSP constitutes a DOE-approved documentation of site contractor safeguards and security operations. Oversight (audits, assessments and inspections) of the contractor must be based upon the approved SSP. If oversight activities identify weaknesses in the approved SSP, associated oversight findings and observations should be directed to the SSP approval authority

Protection programs will be tailored to address specific site characteristics and requirements, current technology, ongoing programs, and operational needs to achieve acceptable protection levels that reduce risks in a cost-effective manner. This baseline level of protection is applicable to all SC Laboratories especially those locations and activities determined to be a SPL 4, (including CAT II SNM)(as described in the DOE O 470.3B, *Graded Security Protection (GSP) Policy,* dated August 12, 2008). For sites with assets with DOE requirements that exceed the baseline, S&S measures in this baseline level of protection should not be applied without consideration of the standards defined in DOE M 470.4-1, Ch2 (as amended), and the appropriate DOE Manuals/Orders for other topical S&S elements and/or National Policy.

Security Areas: Security areas are established to provide protection to S&S interests under SC's purview. These areas and their associated protection measures are established using a graded approach, considering the types of assets involved and the associated protection requirements.

Areas are established and located so that access is the least restrictive and moves inward to the most restrictive level security areas. SC recognizes the following types of areas for the protection of personnel, less-than-Cat II quantities of SNM, and other assets such as classified information and government property.

General Access Area (GAA): These designated areas are accessible to all personnel including the public. DOE line management should establish security requirements for those areas designated as a GAA.

Posting of General Access Areas. The designated GAA security requirements must be posted to inform all personnel, including the public, that entry into these areas subjects them to the security requirements. The posting should list the security conditions (see 41 CFR Part 102-74 Subpart C).

- **Controlled Access Area (CAA):** A CAA is a management defined area that requires some level of controlled access. CAAs include identified boundaries and access control points. CAAs may be established for locations that require access restrictions due to security, safety, specialized training needs, and/or other considerations.

- **Property Protection Area (PPA):** A PPA is a security area established when using, processing, or storing Category IV quantities of SNM, or based on a management determination that increased security is needed beyond that provided by a CAA. PPAs are approved by the contractor and Federal CSAs. PPAs have defined boundaries and access control measures.

- **Limited Area (LA):** An LA is a security area designated for the protection of classified matter and Category III quantities (or higher) of SNM and to serve as a concentric layer of protection. LAs have defined physical barriers, access controls, and other protection measures.

- **Vault Type Room (VTR):** As defined by DOE M 470.4-2A and successor directives. Typically used as secure storage for classified matter.

- **Sensitive Compartmented Information Facility (SCIF):** As defined by DCID 6/9.

Access Control: Access Control is the process of permitting access or denying access to S&S interests, resources, or designated security areas. Each site should maximize the use of automated access control systems for granting entry into security areas and/or access to the assets being protected and minimize the use of personnel to controlled access where missions permit. When possible, a single security badge should be used for access control systems to minimize the number of cards and credentials tracked through the security system. Using automated access controls reserves security personnel for tasks that require interaction such as alarm assessment, fact-gathering, reporting, and incident response. Physical barriers and signage should be used to direct personnel to entry/exit points as necessary.

Badge Program: All sites will implement a consistent badge program that provides the capability to identify authorized persons and determine what the badge holder's authority to be present and/or purpose is at the laboratories. Following is a list of approved badges for access to SC sites and facilities:

- **The SC Badge** - A badge used by uncleared persons authorized by SC for use at designated sites and/or facilities. It may be used for unescorted access to designated SC CAAs and Property Protection Areas (PPAs) (as approved by the CSA and documented in the SSP). It is not authorized at locations that require the DOE Security Badge (such as LA);
- **Local Site-Specific Only (LSSO) Badge** - A badge approved by the DOE CSA for use at a specific local site, only. This includes temporary and visitor badges. It may be used for unescorted access to designated CAAs and PPAs and escorted access to LAs (local site use only as approved by the CSA and documented in the SSP);
- **The DOE Security Badge** - A Homeland Security Presidential Directive-12 (HSPD-12) credential, issued and worn by cleared and specified uncleared individuals as directed by SC for uniformity. This badge may be used for identification or unescorted access to designated SC CAAs and PPAs, as well as access to LAs/VTRs with appropriate need-to-know. There are additional requirements for unescorted access to SCIFs; and
- **Positive Identification** - CAAs do not require use of a badging program, but sites implement requirements to validate identity through use of other identification credentials or means as documented in the SSP.

The appropriate badge should be worn at all times while on the site property (as required per the area designations). An established badge display posture reinforces a positive culture in which security is part of everyone's responsibility. The site population becomes a part of the defense in depth afforded to the site by providing and additional means of detecting those who may not be authorized on site simply by reporting the lack of the appropriate badge being displayed. For example, sites that have all personnel already badged (for S&S areas that do require badges), site SSPs may direct the display of appropriate badges in CAAs as the norm and identify exceptions when unbadged personnel are permitted to traverse or be present in selected CAAs (i.e., open houses, on-site housing, educational outreach events, etc).

Approval Process: Approval processes are the activities undertaken on behalf the CSA to determine whether or not persons requesting entry/access are authorized and meet site requirements established for admission to that specific area. Depending on the area type, requirements may include but are not limited to:

- Verification of identity prior to badge issuance and/or to permit access (i.e., review of official identification credentials);
- Verification of security clearance (as applicable);
- Verification of purpose and/or need-to-know (as applicable);
- Verification of access validity:
  - Programmatic need: Program/project knowledge and approval of visit/access, etc.;
  - Invitation: Open house, job interview, educational outreach programs, and public area management activities, etc.;
- Foreign Visits and Assignments vetting and approvals (as applicable); and
- Escort requirements.

Implementation of an approval process may not always be possible prior to public access to a GAAs, but is required prior to permitting access to CAAs, PPAs, LAs/VTRs, and higher level security areas. GAAs are often "gateways" to the site and site's may incorporate various S&S measures such as signage describing the authority to prohibitarticles and to deny access as determined by the CSA. These measures must be described in the SSP.

Visitor Control: Sites should perform visitor control at the exterior of the site/facility. If this is not possible, it should be performed within the least sensitive area possible (e.g, a GAA or CAA). In no case should visitor control be performed within an LA or more sensitive security area..

Foreign national access to sites, programs, information, and technologies require approval. In accordance with DOE O 142.3A, 4.d., SC laboratories need not perform indices checks for GAA/CAA/PPA access by foreign nationals unless the foreign nationals are nationals of a state sponsor of terrorism, are sensitive country nationals, or the visit involves the discussion of a sensitive subject. Indices are not required for foreign nationals attending public events held onsite or offsite that include only information not protected by statute that is releasable to the general public, held in locations accessible by the public and available for attendance by the general public.

Indices and Secretarial approval is required for visits involving areas other than GAA, CAA, or PPAs and as delineated above. Refer to DOE O 142.3A for specific requirements.

Authentication Process: LAs and above require two-factor authentication for automated access controls to validate both the identity and clearance level of persons seeking unescorted access.
Entry/Exit Screening: The location and scope of the program to screen for prohibited articles at security area boundaries is specified for LAs and above in DOE M 470.4-2A and successor directives. In addition, at SC laboratories, individuals entering and exiting PPAs are subject to inspection to detect prohibited/controlled articles under procedures developed by local security authorities.. Random inspections of individuals entering and exiting LAs (including VTRs/SCIFs) shall be employed to detect prohibited/controlled articles being introduced to the area and security interests being removed without authorization.

Intrusion Detection: Sites should have an intrusion detection capability for LAs/VTRs and SCIFs. LA intrusion detection capabilities can consist of personnel and barriers or storage that provides evidence of penetration of the security area or asset being protected.

The intrusion detection requirements should be determined by the security area type, configuration, construction and vulnerability to postulated threats for the security interest being protected. (See Chapter I, Protection Planning, DOE M 470.4-2A) The IDS should communicate all alarm points to an alarm station.

Alarm Monitoring: An assessment and response capability should be employed for these systems in accordance with the DOE Manuals/Orders. This includes a monitoring station/location to dispatch personnel to the alarm in a timely manner. Depending on the site mission and assets protected, cameras may be used for timely alarm assessment and facilitate appropriate response. The use of cameras for assessment should be documented in the SSP.

For LAs, alarms or notification features of automated control systems (when used) e.g., annunciation of a door alarm, duress, tamper, and door ajar, or anti-pass-back indication feature, should be treated as an intrusion alarm.

Physical Barriers: Barriers typically consist of a coordinated series of natural or fabricated impediments that direct, restrict, limit, delay, or deny entry into a designated area. GAAs and CAAs do not require a physical barrier, but must be posted to inform all personnel, including the public, that entry into these areas subjects them to the security requirements in 41 CFR Part 102-74 Subpart C). PPAs require physical barriers such that they must be crossed, cut, climbed, or breached in a manner that indicates an attempt to enter or depart the area without going through the designated entry and exit control points. The legal boundaries and/or barriers for GAAs, CAAs, and PPAs should be described in the SSP. Barriers for LAs, VTRs, and SCIFs (e.g. fences, walls, doors, windows, ceilings, and floors) are constructed and used to provide evidence of penetration of the security area or access to the security interest being protected. They must provide a degree of barrier delay and meet the requirements set forth in the DOE Manuals/Orders.

Lock and Key Program: A program to protect and manage locks and keys should be established by the CSA. The lock and key program should be applied in a graded manner based on the S&S interests being protected; identified threat, existing barriers, and other protection measures afforded these interests. Security keys include mechanical keys, key cards, and access codes. They are divided into four levels, I through IV based on the S&S interest and/or area being protected. Security keys do not include administrative or privacy lock keys to factory-installed file cabinet locks, desk locks, toolboxes, etc.

- **GAAs and CAAs** - These locations are not required to implement a formal lock and key program, however, at the direction of the CSA, buildings where no classified or SNM is in use or stored may incorporate keys categorized as administrative Level IV.
- **PPAs** - Buildings protecting Category IV quantities of SNM, and/or government property whose loss would adversely impact security and/or site/facility operations should be protected by locks and keys categorized as Level III. Buildings where no classified or SNM is in use or stored may incorporate keys categorized as Level IV.
- **LAs** - Building doors, entry control points, gates, fences, doors, or other barriers or containers protecting Category III SNM and confidential classified matter should be protected by locks and keys categorized as Level II. Locations where top secret and/or secret documents/matter are stored require Level I security locks and keys.
- **VTR and SCIF** - VTRs and SCIFs must be protected by Level I security locks and keys.

All sites should have a lock and key program that manages inventories and tracks Level III and higher keys used to access security areas in accordance with DOE Manuals/Orders. Keys below Level III are not funded as an S&S element.

Response Capability: Each site will maintain a capability for response to site security situations in a timely manner. The response capability should be provided by assigned protective force personnel, by local law enforcement agency, or other authorized and appropriately cleared personnel

as documented in the SSP. The SSP should include the type and number of personnel, weaponry (if applicable), and other equipment. Sites possessing Category I and/or II quantities of SNM or credible roll-up to Category I/II quantities of SNM are required to provide an armed response. Armed response may also be required for SPL 0, 1, 2 and depending upon the consequences SPL 3 level facilities as prescribed in the GSP. All other SC sites require an unarmed response capability. The response capability should provide for augmentation by local law enforcement agencies (documented through Memorandums of Understanding/Agreements) depending on the nature of the security issue/incident and agreements in place.

Deviation from this baseline should be documented through risk assessments. Considerations for such deviations and the risk assessment include the type of response personnel that are available (i.e., armed versus unarmed), the asset location and type, liability issues associated with the site/asset/location, and site threat considerations.

Secure Storage: Each site must manage approved secure storage for the protection of SNM and/or classified matter (e.g., vault, vault-type room, General Services Administration-approved security container, and other selected secure storage containers). Secure storage requirements are delineated through the DOE Orders/Manuals and generally apply within LAs and higher level security areas.

Posting/Signage: Signs should be posted at facilities, installations, and real property based on the need to implement Federal statutes protecting against degradation of S&S interests. Site and security area boundaries should have sufficient demarcation to identify the boundary.

- **GAA/CAA** - The security requirements, including security conditions (as applicable), should be posted to provide reasonable notice to individuals on the general requirements when accessing the area. Signs should be used to direct vehicle and personnel traffic to entry/exit control points at CAAs.
- **PPA** - Signs prohibiting trespassing, listing prohibited articles, and that video surveillance equipment is in use (if applicable), should be posted at the perimeter and at entrances in accordance with the DOE Manuals/Orders. Additional signs may be posted at inner security areas (i.e., LAs within PPAs) at the discretion of the CSA.
- **LA (including VTRs/SCIFs)** - Signs to convey information on prohibited and controlled articles, the inspection of vehicles, packages, hand carried items, personnel entering and exiting the area, no trespassing, and that video surveillance equipment is in use (if applicable) must be posted in accordance with the DOE Manuals/Orders.

Training: Federal and contractor staff and visitors should receive appropriate security briefings and/or training. Protection of personnel and property is everyone's business. An initial security briefing is required for all contractor employees or personnel who receive a badge providing unescorted access to security areas.

Security Conditions (SECON): A progressive level of common sense protective measures that may be implemented in response to a malevolent or terrorist threat to any or all DOE facilities, assets, and personnel. Once a SECON level is declared, the associated protective measures should be implemented as soon as possible to the extent they apply to the individual site or facility. CSAs should coordinate SECON status through their DOE points of contact. Measures associated with each SECON listed in DOE Manuals/Orders are not prioritized but should be initiated concurrently when practical in accordance with CSA direction. The implementation of SECON measures listed in DOE directives must be described in the SSP.

SC S&S Baseline Level of Protection by Security Area						
S&S Element	**General Access Area (GAA)** Accessible to all personnel and the public	**Controlled Access Area (CAA)** Management defined area including entry point that requires controlled access beyond a GAA	**Property Protection Area (PPA)** Established when using, processing, storing CAT IV SNM or based on management determination of the need for increased security not provided by a CAA	**Limited Area (LA)** Designed for the protection of classified matter and CAT III or higher SNM as a concentric layer of protection	**Vault Type Room (VTR)**	**Sensitive Compartmented Information Facility (SCIF)**
Security Plans	For all areas, the rationale for their establishment, protected contents, entry requirements, and physical barriers, additional controls such as training, boundaries, and unique considerations must be clearly described in the Site Security Plan (SSP).					
Entry and Access Control Elements						
Security Clearance	Not required for these areas			Required for unescorted entry and "access"		
Badge types	**Areas where badges are required for unescorted entry**					
1. DOE HSPD-12 badge	Not required for these areas		Permits unescorted entry	Permits entry (with additional requirements)		
2. SC badge, LSSO, Temporary, Foreign National and Visitor	Not required for these areas		Permits unescorted entry	Unescorted entry not permitted with these badges		
Approval Process e.g. training, need to know, foreign national vetting, open house	Not required	Required for entry to all areas except GAAs				
Authentication Process e.g. biometric, PIN, personal verification, escort, etc.	Not required for these areas			Required	Required	Required
Positive ID	Not required	Required	**Badge** required for entry into these areas			
Physical Security Elements						
Designated Entry Point	Not required	Required	Required	Required	Required	Required
Intrusion Detection System	Not required for these areas			Not required but when Automated access control (AAC) is used, it must act as IDS for the entryway	Required w/access logging	Required
Barriers	Not required		Required	Required	Required	Required
Lock and Key	Not required		Required	Required	Required	Required
Response Capability	Not required		Not required for a PPA	Required	Required	Required
Storage Areas	Not required		Not required for a PPA	Required		
Alarm Monitoring	Not required for these areas			Not required but when Automated access control (AAC) is used, it must act as IDS for the entryway	Required	Required
Posting/Signage	Required for all areas					
Training	Not required		Required	Required	Required	Required

This page intentionally left blank