
**OFFICE OF CYBER SECURITY
AND SPECIAL REVIEWS**

APPRAISAL PROCESS GUIDE



NOVEMBER 2001

**U.S Department of Energy
Office of Cyber Security and Special Reviews
19901 Germantown Road
Germantown, Maryland 20874**

Preface

The Office of Independent Oversight and Performance Assurance (OA) published an Appraisal Process Guide to describe the philosophy, scope, and general procedures applicable to all independent oversight appraisal activities. The Office of Cyber Security and Special Reviews (OA-20) is one of five subordinate offices of the OA. This Appraisal Process Guide was prepared to provide additional information and detail about the appraisal approach and techniques specific to OA-20. There are also other references that provide insight into the OA-20 approach to independent oversight activities. The Office of Cyber Security and Special Reviews Appraisal Process Guide should be used along with the OA Appraisal Process Protocols, the Office of Safeguards and Security Evaluations (OA-10) Safeguards and Security Appraisal Process Guide, and DOE Order 470.2A, *Security and*

Emergency Management Independent Oversight and Performance Assurance Program, to provide an understanding of the general processes and activities associated with evaluations of classified and unclassified cyber security programs throughout the U.S. Department of Energy (DOE).

As part of the continuing efforts to improve the independent oversight process, OA-20 anticipates making periodic updates and revisions to this appraisal guide in response to changes in DOE program direction and guidance, insights from independent oversight activities, and feedback from customers and stakeholders. Therefore, users of this document, as well as other interested parties, are invited to submit comments and recommendations to the Office of Cyber Security and Special Reviews.

This page intentionally left blank.

Contents

Acronyms	v
Definitions	vi
Section 1. Introduction.....	1
Mission	1
About This Guide	2
Scope of Cyber Security Appraisals and Special Reviews	2
Program Reviews	2
External Network Security Assessments	2
Special Reviews.....	3
Section 2. Approach.....	5
Introduction	5
Approach to Cyber Security Appraisal Activities.....	5
Appraisal Goals and Philosophy	7
Roles and Responsibilities	7
Compliance Versus Performance	8
Local Representatives	9
Appraisal Standards	9
Section 3. Planning	11
Introduction	11
Goal	12
Preplanning Phase	12
Planning Phase	12
Performance Test Agreement	13
Document Requests for Cyber Security.....	13
Inspection Plan.....	14
Onsite Inspection Schedule.....	14
Planning Products.....	15
Field Augmentation Program	15
Section 4. Conduct.....	17
Introduction	17
Goal	17
Performance Testing	17
Programmatic Review	18
Communications and Feedback.....	18
Section 5. Closure.....	21
Introduction	21
Goal	21
Analysis of Results.....	21

Contents (Continued)

Findings 22
Explanation of Rating System 22
Report Preparation 22
Quality Review Board 22
Briefings 22
Process Improvements 23
Documentation of Appraisal Activities 23

Section 6. Follow-Up 25

 Introduction 25
 Goal 25
 Headquarters Briefings 25
 Final Reports 25
 Corrective Action Plans 26
 Corrective Actions and Follow-Up 26

Appendix A: Cyber Security Performance Testing Approach A-1
Appendix B: Cyber Security Program Evaluation Framework B-1
Appendix C: Reference Documents C-1
Appendix D: Sample Independent Oversight Cyber Security Performance Test Agreement D-1
Appendix E: Summary Sheets for Interviews Conducted and Key Documents Reviewed E-1

Acronyms

CIAC	Computer Incident Advisory Capability
CSPP	Cyber Security Program Plan
DCSM	Departmental Cyber Security Management Policy
DOE	U.S. Department of Energy
DNS	Domain Name Server
IG	Office of the Inspector General
IP	Internet Protocol
ISS	Internet System Scanner
ISSM	Integrated Safeguards and Security Management
OA	Office of Independent Oversight and Performance Assurance
OA-10	Office of Safeguards and Security Evaluations
OA-20	Office of Cyber Security and Special Reviews
PBX	Private Branch Exchange
SSIMS	Safeguards and Security Information Management System

Definitions

Appraisal – An umbrella term for any oversight activity conducted by the Office of Independent Oversight and Performance Assurance. Inspections, special inspections, assessments, special studies, and special reviews are all forms of appraisals.

Corrective Action Plan (CAP) – A document that provides, for each finding or deficiency addressed, planned corrective actions, the responsible person(s) and organizations; the date of action initiation; key milestones; the date of expected completion of the action; how actions will be tracked to closure; steps to address root causes and generic applicability; and the mechanism(s) for verifying closure and ensuring that actions are sufficient to prevent recurrence. May also include a detailed discussion of longer-term enhancements and upgrades, as well as descriptions of actions taken and compensatory measures already in place.

Cyber System – Any computer or network device that communicates, manipulates, monitors, stores, or transmits U.S. Department of Energy information. Also known as an information technology system.

Cyber Security – The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained within computer networks and systems, as well as measures designed to prevent denial of authorized use of the system.

Deficiency – An inadequacy that is found during an inspection and is listed for corrective action.

Finding(s) – Concise, factual statement(s) of key observations and conclusions resulting from an oversight activity.

Performance Testing – The evaluation of all or selected information technology systems by direct experimentation over the Internet or from within a network to test the effectiveness of established cyber security protection measures.

Programmatic Review – The evaluation of all or selected portions of essential underlying cyber security management processes that are fundamental to a sound program.

Section 1

INTRODUCTION

Contents

Mission	1
About This Guide	2
Scope of Cyber Security Appraisals and Special Reviews.....	2
Program Reviews	2
External Network Security Assessments.....	2
Special Reviews	3

Mission

The Office of Independent Oversight and Performance Assurance (OA) is charged with conducting appraisals of safeguards and security, cyber security, emergency management, and environment, safety, and health programs at U.S. Department of Energy (DOE) sites for the Secretary of Energy. As such, OA provides DOE and contractor line managers, Congress, and other stakeholders with an independent evaluation of the effectiveness of safeguards and security; cyber security; emergency management; and environment, safety, and health policies and programs and their implementation (Reference DOE Order 470.2A, *Security and Emergency Management Independent Oversight and Performance Assurance Program*). For each of these areas, OA follows a common set of overall appraisal protocols as described in the Office of Independent Oversight and Performance Assurance Appraisal Process Protocols.

This document, Office of Cyber Security and Special Reviews Appraisal Process Guide, provides additional insight into OA's evaluation approach and processes associated with assessing classified and unclassified cyber security programs. The objective of this document is to establish a standard approach and methodology for conducting cyber security reviews that is well understood by all inspection participants.

The Office of Cyber Security and Special Reviews (OA-20) is responsible for implementing the independent oversight function of the DOE in matters related to cyber security. The activities of OA-20 encompass:

- Periodic inspections of classified and unclassified cyber security programs at DOE sites
- A continuous program of remote testing for DOE network vulnerabilities through scanning and penetration testing
- Follow-up activities to ensure that identified issues are addressed in a timely and effective manner
- Studies of cyber security issues across the DOE complex
- Development of recommendations and identification of opportunities for improving cyber security performance
- Review of other governmental and commercial cyber security programs to provide benchmarks for DOE performance
- A “rapid response” capability to perform special reviews for the Secretary of Energy and senior DOE managers
- Ongoing analyses to identify trends and emerging issues in the cyber security arena
- Assessments of the effectiveness of DOE policies governing classified and unclassified cyber security
- Inputs for the annual evaluation of DOE’s unclassified information security programs as required by the Government Information Security Reform Act

Introduction

- Annual evaluations of classified information security programs for DOE as required by the Government Information Security Reform Act.

About This Guide

This Office of Cyber Security and Special Reviews Appraisal Process Guide is a subordinate document to the OA Appraisal Process Protocols. While the OA Appraisal Process Protocols provide general guidance common to all appraisal activities, this document provides additional detail and guidance regarding procedures and methods specific to cyber security appraisals conducted by OA-20. Another important companion document used by OA-20 is the Safeguards and Security Appraisal Process Guide published by the Office of Safeguards and Security Evaluations (OA-10). The majority of OA-20 inspection activities are conducted jointly with OA-10 as safeguards and security inspections. The Safeguards and Security Appraisal Process Guide provides guidance on the conduct of safeguards and security evaluations by OA-10 and OA-20 inspectors. DOE Order 470.2A is an important reference document that defines program requirements and, in particular, defines how sites should respond to identified vulnerabilities and the corrective action plan development process. Since all these documents should be used together, every effort has been made to avoid unnecessary duplication. For that reason, text in this guide sometimes refers to sections or appendices of these other documents. OA-20 inspectors should maintain familiarity with information in all of these documents.

This guide focuses on the inspection process, including program reviews, external network security assessments, and special reviews. OA-20 inspectors may also conduct other appraisals and special studies as necessary. While those types of appraisals are not specifically addressed in this guide, the processes associated with those activities differ only in detail. For example, the appraisal phases and the types of activities associated with each phase generally apply; similar data collection methods are used; and validation, analysis, and

report-writing requirements are similar. When the specific needs of a review or special study require a significant deviation from the process, methods, and techniques described in this guide, OA-20 will develop a project plan to guide the appraisal or special study.

Scope of Cyber Security Appraisals and Special Reviews

To carry out assigned responsibilities, OA-20 inspectors conduct various types of appraisals, including program reviews, external network security assessments, and special reviews. The type and frequency of scheduled reviews are based on overall OA protocols for prioritization.

Program Reviews

- **Inspections** encompass a full programmatic review of all elements of classified and unclassified cyber security programs and include extensive external and internal performance testing.
- **Focused reviews** assess the effectiveness of one or more aspects of a site's classified and/or unclassified cyber security program up to the scope of an inspection. A focused review normally includes a performance testing component.
- **Follow-up reviews** assess the status of corrective actions identified during either an inspection or a focused review. Performance testing may be conducted to verify the effectiveness of corrective actions.
- **Unannounced inspections** can be of varying scope. As defined, the key aspect is that the site is not informed of the inspection beforehand. However, if any unannounced performance testing is involved, OA-20 will work with "trusted agents" at the site to coordinate activities.

External Network Security Assessments

External network security assessments focus on remote announced performance testing via the Internet to systematically probe a site's network perimeter, identify vulnerabilities, and evaluate the potential for exploitation. All assessment

activities are conducted remotely from OA-20's cyber security laboratories. OA-20 external network security assessments consist of:

- Scanning network systems exposed to the Internet for vulnerabilities and attempting exploits to evaluate the potential impact of weaknesses
- Tabletop reviews of firewall rules and border router access control lists to identify potential weaknesses associated with allowed services and trust relationships
- Tabletop reviews of intrusion detection parameters and system architecture to evaluate the site's capability to detect intruders and mitigate vulnerabilities
- Scanning site telephones using a war-dialer to identify unauthorized or misconfigured modems that could provide an alternative route into the network.

External network security assessments do not involve an onsite programmatic review or internal performance testing and, as a result, do not provide a complete picture of performance or an evaluation of the direction of the program. However, such assessments do provide a "snapshot in time" of the effectiveness of a DOE site's network perimeter defense strategy. These assessments were designed to provide independent oversight coverage at lower priority sites that may not otherwise be scheduled for another type of cyber security appraisal by OA. Because these activities are conducted remotely,

OA-20 is able to stretch existing resources to provide valuable feedback to a greater number of DOE sites.

Tabletop reviews, technical interviews, and factual accuracy reviews associated with an external network security assessment are generally conducted via conference call. OA-20 does make a site visit at the end of the assessment to brief the site management on the results of the performance testing, as well as engage site personnel in additional technical discussions. External network security assessments are generally not rated; however, findings may be issued.

Special Reviews

Special studies and reviews conducted by OA-20 focus on crosscutting cyber security functions and issues. This type of appraisal is particularly well suited to assess the effectiveness of protection strategies for information systems that cross physical site boundaries. Additionally, specific issues with broad applicability to DOE can be analyzed. Special studies and reviews typically include multiple sites allowing OA-20 personnel the opportunity to gather sufficient data to allow broad conclusions with applicability to the entire DOE complex. Special reviews can involve subject matter experts from the field, DOE Headquarters organizations, other government agencies, and the private sector.

This page intentionally left blank.

Section 2

APPROACH

Contents

Introduction.....	5
Approach to Cyber Security Appraisal Activities	5
Appraisal Goals and Philosophy.....	7
Roles and Responsibilities.....	7
Compliance Versus Performance.....	8
Local Representatives.....	9
Appraisal Standards.....	9

Introduction

The OA-20 appraisal program provides a practical approach to assessing cyber security throughout the DOE complex. Processes are constantly reviewed, refined over time, and applied according to the degree of protection needed. Processes, procedures, and tools used are also adjusted, modified, and updated to keep current with the threats that new cyber technology introduces. This allows OA-20 to use government and industry best practices to ensure that cyber security is appropriately applied to ensure that adequate protection measures are established for a secure operating environment.

OA-20 has established a systematic approach for cyber security appraisal activities that includes performance testing and a review of key program elements in order to conduct thorough and objective assessments. Team members use a variety of performance tests and implementation assessments to evaluate and identify strengths and weaknesses in cyber security implementation. Performance testing provides a good snapshot of the effectiveness of performance but does not provide insight into the sustainability and direction of the program. Additionally, technical weaknesses that are identified through performance testing are generally symptoms of larger, more pervasive problems associated with management of the

site's cyber security program. Therefore, OA as a whole places significant emphasis on complementing technical performance testing with a programmatic review to assess the effectiveness of key underlying management processes associated with cyber security programs. This results in identification of systemic issues and provides a basis for evaluating the direction and sustainability of cyber security programs.

As described in the Appraisal Process Protocols, all OA appraisals have four major phases: (1) Planning, (2) Conduct, (3) Closure, and (4) Follow-up. These four phases, as they relate to cyber security appraisals, are described in Sections 3 through 6 of this Guide.

Approach to Cyber Security Appraisal Activities

To conduct thorough and objective evaluations, OA-20 has established a systematic approach for its evaluation activities. OA-20 protocols are consistent with DOE's *Integrated Safeguards and Security Management (ISSM) Policy*, DOE Policy 470.1, and the *Departmental Cyber Security Management (DCSM) Policy*, DOE Policy 205.1, which further clarifies the ISSM policy for implementing cyber security. The ISSM and DCSM policies contain guiding principles and core functions that establish a framework for integrating cyber security into

Approach

management and work practices to protect classified and unclassified information processed on computer and network systems. The ISSM/DCSM guiding principles and core functions are shown in Table 1.

To fully evaluate the integration of cyber security into management and work practices, OA-20 cyber security inspection activities involve a combination of performance testing and a programmatic review of essential elements that form the foundation of an effective program. OA-20 technical team personnel conduct extensive internal and external performance testing to evaluate the effectiveness of protection measures for classified and unclassified networks. When technical implementation issues are identified, they can generally be seen as symptoms of larger, more pervasive problems in the management and implementation of the site program. The programmatic review uses the results from performance testing as a basis to identify strengths and weaknesses of program implementation as well as underlying root causes.

OA-20 utilizes a Technical Standard Operating Procedure to ensure a consistent technical approach to cyber security performance testing. This is an internal OA-20 document that defines

the step-by-step approach to internal and external performance testing as well as information that is collected and retained during performance testing activities. An overview of OA-20's approach to performance testing activities is provided in Appendix A.

OA-20 programmatic reviews are focused on both program direction and program implementation. Program direction is evaluated by assessing how well both DOE and contractor line management satisfy key responsibilities. There is a strong link between these responsibilities and the guiding principles of ISSM/DCSM. Program implementation is evaluated using an evaluation framework identical to the five core functions of ISSM/DCSM. Appendix B contains this evaluation framework, which is utilized for cyber security program reviews along with general lines of inquiry.

OA-20 cyber security inspection results are routinely presented around the framework described in Appendix B. This framework is not intended for use as an evaluation checklist; rather, it is to be used as a guide to help the OA-20 inspection team conduct a thorough assessment that identifies both positive aspects of program direction and implementation as well as barriers to effective performance. OA-20

Table 1. ISSM/DCSM Guiding Principles and Core Functions

ISSM/DCSM Guiding Principles
<ul style="list-style-type: none"> • Individual responsibility and participation • Line management responsibility for safeguards and security/cyber security • Clear roles and responsibilities • Competence commensurate with responsibilities • Balanced priorities • Identification of safeguards and security standards and requirements • Tailoring of protection strategies to work being performed
ISSM/DCSM Core Functions
<ul style="list-style-type: none"> • Define the scope of work • Analyze the risk • Develop and implement security measures • Perform work within measures and controls • Provide feedback and continuous improvement

teams also use the framework to help structure interviews, data collection, analysis, and other inspection activities.

Appraisal Goals and Philosophy

The OA oversight goals and philosophy stated in OA Appraisal Process Protocol Section 2 are adopted by OA-20 to guide appraisal activities.

Roles and Responsibilities

To ensure that planning, conduct, closure, and follow-up activities are accomplished effectively and efficiently, key functions and tasks are assigned to various positions based on OA-20 organizational and assessment assignments.

Director, Office of Cyber Security and Special Reviews

The Director of OA-20 has responsibility for the following key functions and tasks:

- Implement OA cyber security appraisal program
- Provide overall direction and guidance
- Establish appraisal schedules
- Interface with Headquarters and field personnel to coordinate activities and address concerns
- Serve as Inspection Team Chief for safeguards and security inspections when designated by the Director, Office of Independent Oversight and Performance Assurance
- Make cyber security appraisal team assignments and establish review scope
- Participate on Quality Review Board
- Brief senior DOE management and other stakeholders on appraisal results.

Deputy Director, Office of Cyber Security and Special Reviews

The Deputy Director of OA-20 has responsibility for the following key functions and tasks:

- Provide direction and guidance consistent with the OA-20 Director
- Recommend appraisal schedules
- Serve as Inspection Team Chief for safeguards and security inspections when designated by the Director, Office of Independent Oversight and Performance Assurance
- Support OA-20 Director in interfacing with Headquarters and field personnel to coordinate activities and address concerns
- Recommend appraisal team structure and scope
- Participate on the Quality Review Board as requested
- Brief senior DOE management and other stakeholders on appraisal results.

Team Leader/Topic Team Leader (for Safeguards and Security Inspections)

The OA-20 Team Leader/Topic Team Leader has responsibility for the following key functions and tasks:

- Lead appraisals of cyber security programs or topics
- Provide input on recommended appraisal scope
- Provide direction and guidance to team members on the approach to specific appraisal activities
- Draft cyber security portion of inspection plan
- Provide feedback on proposed appraisal team structure and make recommendations for additional resources needed to accomplish scope
- Make arrangements with the site for document requests and other logistics as needed
- Establish the schedule of events for cyber security appraisals and make specific assignments
- Ensure that team members perform their assigned duties
- Address site concerns associated with appraisal activities

Approach

- Provide feedback to site personnel on a daily basis to validate assessment information and clearly communicate areas of concern
- Prepare and present appraisal reports
- Brief site management and cyber security personnel on appraisal results.

Technical Lead

The OA-20 Technical Lead has responsibility for the following key functions and tasks:

- Support Team Leader/Topic Team Leader in leading appraisals of cyber security programs or topics
- Provide input on recommended appraisal scope
- Provide direction and guidance to team members on the approach to cyber security technical performance testing
- Provide input to the Team Leader/Topic Team Leader on document requests and other necessary logistics to support the technical team
- Provide feedback on proposed cyber security appraisal team structure and make recommendations for additional resources needed to accomplish scope
- Establish the cyber security technical assessment schedule and make specific assignments
- Ensure that technical team members perform their assigned duties
- Address site concerns associated with technical performance testing activities
- Provide feedback to site personnel on a daily basis to validate assessment information and clearly communicate areas of concern
- Prepare and present cyber security technical appraisal reports
- Participate in briefing site management and cyber security personnel on appraisal results.

Team Member(s)

An OA-20 Team Member has responsibility for the following key functions and tasks:

- Support the Team Leader/Topic Team Leader and Technical Lead in conducting appraisals of cyber security programs or topics
- Provide input to the Team Leader/Topic Team Leader and Technical Lead on appraisal scope and potential approaches for accomplishing cyber security appraisals
- Conduct appraisal activities following direction and guidance of Team Leader/Topic Team Leader or Technical Lead
- Prepare the schedule of interviews to accomplish during onsite visit
- Review key site cyber security documents prior to the onsite visit
- Conduct thorough and fair appraisals
- Validate assessment data and conclusions with site personnel on a daily basis to ensure factual accuracy
- Provide written input for draft appraisal reports as directed by the Team Leader/Topic Team Leader and Technical Lead
- Participate in briefing site management and cyber security personnel on appraisal results.

Compliance Versus Performance

DOE cyber security policy requires that certain functions be performed and that certain levels of protection be achieved. However, policy does not always contain specific measures that must be taken or indicate how to achieve an appropriate level of protection. Therefore, to effectively evaluate the adequacy of cyber security protection, OA-20 takes a performance-based approach rather than solely a compliance-based approach to appraisals. Findings, linked to broad policy requiring the protection of DOE information technology systems, are issued to line management if an appraisal identifies significant weaknesses that contribute to inadequacies in cyber security protection.

OA-20 does assess the extent to which DOE sites comply with current program requirements and reports any significant cases of non-compliance, while also setting forth mitigating circumstances and providing an analysis of whether program objectives have been met and

maintained. If DOE establishes a new policy which has not yet been incorporated into a contract as a binding requirement, then OA-20 will not hold the site accountable for compliance with that requirement. DOE line management may receive a finding for not incorporating the requirement in a timely manner if appropriate. However, if lack of implementation of that requirement adversely impacts protection, a finding may also be issued to the site as a performance issue.

Mitigating factors might exist for both compliance and performance issues. For example, deficiencies in program or system performance might be mitigated by the existence of alternative processes or controls, such as:

- Alternative documentation indicating that required functions were performed, factors were considered, or decisions were made
- Risk assessments and acceptance by the appropriate level of management
- Complementary procedures or features that function effectively
- Demonstration through performance testing that DOE assets are afforded a level of protection equivalent to that specified by DOE directives.

Local Representatives

The cooperation and assistance of DOE site representatives is essential to ensuring that a full and accurate cyber security appraisal is conducted. Local representatives provide detailed site and systems knowledge, arrange administrative and logistical support, expedite appraisal activities, and provide valuable feedback on factual accuracy.

Relations between the appraisal team and local representatives should be cordial, open, and

professional to provide maximum value. It is in the interest of both OA-20 and the local representatives to approach cyber security appraisals in partnership to ensure that these activities result in better protection levels for DOE information technology resources.

Appraisal Standards

OA-20 appraisals are based on national standards, public laws, executive orders, and DOE directives with which DOE cyber security protective programs must comply. The President, Congress, DOE, and other executive offices establish these requirements. As stated previously, OA-20 evaluates compliance with these requirements in the context of a performance-based review that uses extensive performance testing. The list of policies that OA-20 may reference is contained in Appendix C. While the evaluation framework used by OA-20 for programmatic reviews (see Appendix B) is focused on performance, it also has a strong basis in the requirements established by this list of policies. As part of OA-20's responsibility to evaluate the effectiveness of DOE cyber security policy, a finding may be issued against a Headquarters organization for the lack of effective policy in an area.

Local standards are those imposed by the local DOE site, facility contractor, or subordinate contractors responsible for both the site and for administering cyber security. Local standards usually deal with site-specific implementation of national requirements, and might be more stringent. The local standards are communicated through site instructions, procedures, and through the Cyber Security Program Plan (CSPP). The effectiveness of local standards is evaluated during the course of onsite programmatic reviews.

This page intentionally left blank.

Section 3

PLANNING

Contents

Introduction.....	11
Goal.....	12
Preplanning Phase.....	12
Planning Phase.....	12
Performance Test Agreement.....	13
Document Requests for Cyber Security.....	13
Inspection Plan.....	14
Onsite Inspection Schedule.....	14
Planning Products.....	15
Field Augmentation Program.....	15

Introduction

This section is written with an OA safeguards and security inspection in mind. For different types of appraisal activities, the preplanning and planning phases are adapted based on the nature and extent of the planned activity. For example, an external network security assessment that is conducted remotely and consists only of performance testing requires much less planning than a full inspection.

When scheduling an inspection, an initial step involves identifying and assigning resources for the activity. The OA-20 Director designates a Team Leader/Topic Team Leader and Technical Lead. Working with the Technical Lead, the Team Leader/Topic Team Leader plans the conduct of the appraisal and closely coordinates with the OA-20 Director to ensure the thoroughness and rigor of the inspection.

During OA safeguards and security inspections that involve a joint appraisal with OA-10, the OA-20 Team Leader/Topic Team Leader will also operationally report to the Inspection Team Chief. The Director of the Office of Independent Oversight and Performance Assurance (OA-1) designates an Inspection Team Chief for the inspection, who serves as the

senior DOE official managing the evaluation activities and the senior OA point of contact with the site being inspected. The Inspection Team Chief might be from OA-10, OA-20, or even another OA office for combined appraisal activities. In any case, the Inspection Team Chief, OA-20 Director, and OA-20 Team Leader/Topic Team Leader are responsible for closely integrating activities into a single inspection activity. During joint inspection activities, OA-20 will follow general appraisal procedures established by OA-10 and documented in the Safeguards and Security Appraisal Process Guide.

The OA-20 Team Leader/Topic Team Leader serves as the primary point of contact to DOE and contractor mid-level managers at the site on matters related to the cyber security aspects of the inspection. The OA-20 Technical Lead is responsible for the planning and conduct of the technical aspects of the inspection, such as external performance testing (including penetration testing), internal performance testing, and tabletop reviews. The Technical Lead works with the OA-20 Director to develop a performance test agreement that the OA-20 Director, DOE Operations/Site Office representative, and the site contractor representative sign. The performance test

Planning

agreement is discussed in more detail below. Team members are assigned to support the programmatic and technical review as needed.

For integrated appraisals, the Inspection Team Chief will be the primary point of contact for the OA team and will make the necessary arrangements with the site for space, logistics, and other common team needs. For an OA-20-only appraisal, the Team Leader/Topic Team Leader will pick up these responsibilities. What follows are the specific aspects unique to planning the cyber security portion of an appraisal that will normally be handled through the OA-20 Team Leader/Topic Team Leader and/or Technical Lead.

Goal

The goal of planning is to identify and prepare for the actions necessary to conduct an effective and efficient cyber security appraisal of the site's management and technical program.

Preplanning Phase

Preplanning activities are initiated by the Director of OA-20 or the Inspection Team Chief with the senior Federal or contractor site manager to establish high-level agendas, appraisal parameters, and site and inspection team points of contact. There is close coordination between the Director of OA-20 and the Inspection Team Chief for joint OA-10 and OA-20 appraisals to ensure that preplanning activities are effectively conducted.

The OA-20 team conducts preplanning by becoming familiar with the site organization, reviewing documentation, and developing an approach to the appraisal. There also may be a preplanning meeting that includes key team members at the Germantown Headquarters building to assist in focusing the upcoming appraisal. Preplanning activities include:

- Establishing appraisal parameters
- Reviewing available facility information (including past reports, corrective action plans, etc.)
- Identifying appraisal focus areas

- Identifying cyber systems that will be assessed
- Preparing an inspection plan
- Developing a request to the site for documentation
- Establishing a performance test agreement
- Establishing site points of contact
- Coordinating logistics with site personnel (including site access issues, training requirements, team space, and support needs)
- Planning travel and lodging arrangements for team members.

Planning Phase

After completing the preplanning activities, detailed appraisal planning begins. Although a scope is established in the inspection plan, changing circumstances may warrant modifications; thus, flexibility should always be maintained. OA-20 routinely begins performance testing during the planning phase of the inspection after the performance test agreement is signed. This allows the inspection team to collect critical performance testing data to support the programmatic review during the conduct phase of the appraisal.

Planning activities include:

- Reviewing information provided by the site in response to the team's data call
- Understanding the organizational structure and identifying key personnel to interview
- Translating the assessment scope (including focus areas) into a specific approach (i.e., conducting detailed planning)
- Identifying potential problem areas
- Conducting internal and external network performance testing
- Developing interview schedules for the onsite programmatic inspection
- Finalizing logistics arrangements.

A planning week may be scheduled at the site to allow appraisal team members to meet key site personnel, conduct network performance testing, review site documentation, conduct exploratory interviews, and determine how key areas can be

assessed effectively. At the conclusion of the planning week, a brief is provided to the OA-20 Director and the Inspection Team Chief (for joint OA-10 and OA-20 inspections) on progress and specific approaches.

Performance Test Agreement

In preparation for performance testing, a performance test agreement is developed that explains the general approach and defines specific parameters and controls that will be followed during testing. Appendix D contains an example of a performance test agreement. The performance test agreement must be signed by the OA-20 Director, a designated Federal representative, and a contractor representative (if appropriate) prior to beginning any performance testing. All performance test agreements include the following general controls that OA-20 follows:

- Protect all information (classified and unclassified) from unauthorized access in accordance with DOE orders
- Suspend testing at the request of the site if there are legitimate safety, security, or operational concerns
- Maintain frequent communications with the site on the status of testing activities
- Upon completion of testing, work with the site and provide detailed information to return computer systems to their original configuration so that no systems are left in a compromised condition
- In the unlikely event that performance testing adversely affects an information system, work with the site to determine the nature of the problem and restore the system to its desired state of operation
- Inform the DOE Computer Incident Advisory Capability (CIAC) of performance testing to ensure that testing activities are not confused with real attacks.

As part of establishing a performance test agreement, the site is responsible for informing OA-20 if certain critical systems, such as safety systems or major business applications, are undergoing upgrades or should be excluded

from testing activities. In addition, the site must identify any system that is connected to the site network, but is not under the direct control and responsibility of the site. Based on this information, OA-20 may exclude some cyber systems from performance testing activities. OA-20 also conducts performance testing of phone systems to look for backdoors into the site's network. As with cyber systems, specific telephone systems may be excluded from OA-20 performance testing based on valid requests or if the system is not under the control of the site.

Document Requests for Cyber Security

Technical Data Call. To support cyber security performance testing, the OA-20 inspection team will request various documents and items of information. OA-20 typically requests the following types of technical data:

- Technical points of contact for network and computer systems and the phone system; should include office telephone numbers, e-mail addresses, and off-hour contact information
- Internet protocol (IP) addresses for all site computers that include addresses exposed to the Internet, as well as any address ranges on restricted or "yellow" networks
- List of systems within the site address range that are requested to be excluded for safety, security or other reasons; should include the IP addresses and the reasons for exclusion
- List of site phone numbers or phone number ranges
- List of phone numbers to be excluded and rationale as discussed above
- Network topology map containing perimeter devices and IP addresses of those devices, including main border router, other routers that have separate Internet connections, firewalls, gateways, and major subnet routers
- Router access control lists and firewall rules (provided after conclusion of penetration testing)
- Diagram of the classified computer network(s).

Programmatic Review Document Request.

The OA-20 inspection team requests documents from the site during the planning and conduct phases of the inspection to gain an understanding of the site's cyber security program. Document requests typically include:

- CSPP and other relevant site-specific management documents
- Security plans or master plans that describe the cyber security protection measures for computer systems, facsimiles, printers, and other devices processing classified information
- Organizational charts including names and phone numbers of individuals with a role in the site's cyber security program, and primary points of contact for team members
- Copies of recent assessments, surveys, self-assessments, and reviews for classified and unclassified cyber security programs
- Any documentation on cyber security lessons-learned program
- Issue tracking reports and corrective action plans
- Site-specific threat assessment information
- Risk assessment documents
- Documented risk mitigation strategies
- Integrated Safeguards and Security/Departmental Cyber Security Management policy implementation plans
- Results of the most recent site external and internal vulnerability scans
- List of classified computers and networks, including accreditation plans and data
- List of systems processing sensitive unclassified information and the nature of the sensitivity (e.g., Unclassified Controlled Nuclear Information, Official Use Only, and Privacy Act)
- List of computer system incident reports for classified and unclassified systems over the past two years
- Cyber security metrics/performance for the past two years
- Budget prioritization documentation
- Site cyber security policies and procedures
- Documents that explain cyber security training program objectives for users and cyber security professionals.

Inspection Plan

For each inspection, OA-20 develops an inspection plan that describes the team's general scope and approach to conducting the appraisal, defines any specific focus areas, lists team members, and establishes basic ground rules for conducting the overall inspection. In those cases where OA-20 conducts joint inspection activities with OA-10, a joint inspection plan will be developed by the Inspection Team Chief with input from the OA-20 Team Leader/Topic Team Leader and concurred upon by the OA-10 and OA-20 Directors. Although the inspection team is not limited to evaluating specific areas in the inspection plan, every effort is made to identify areas of emphasis during the inspection. A copy of the inspection plan, once approved by OA-1, is sent to the site prior to the onsite appraisal.

Onsite Inspection Schedule

To efficiently use the limited time on site and ensure a thorough appraisal, each team member develops an inspection schedule that addresses the critical data collection activities needed to satisfy the scope defined in the inspection plan. Some flexibility is built into inspection schedules to allow additional interviews to be added after arrival at the site to fill data gaps or clarify information. The development of the inspection schedule requires extensive coordination with the site to set up interviews, walkthroughs, tabletop reviews, and validation meetings.

On a daily basis, the OA-20 inspection team will schedule informal validation meetings with site cyber security staff to provide feedback on the progress of data collection, areas requiring further review, and issues of potential concern, if any. Additionally, a management meeting with the security director or the chief information officer is held each day to briefly discuss the progress of the programmatic review and performance testing. For joint OA-10 and OA-20 activities, the Inspection Team Chief is responsible for conducting the management meeting. The Team Leader/Topic Team Leader may also be needed for this meeting at the discretion of the Inspection Team Chief.

Planning Products

Products resulting from the inspection team's preplanning and planning efforts include:

- Performance test agreement
- Inspection plan that includes identification of focus areas and team roster
- Document request list and subsequent data call provided by the site
- List of site points of contact
- Logistics and travel plans (normally documented in a memo sent to team members)
- Detailed schedule of interviews for onsite inspection.

Field Augmentation Program

A field augmentation program has been established that allows qualified Federal and contractor personnel from Headquarters and the field to participate as members of OA inspection teams. The purpose of OA's program is to help improve the performance of safeguards and security, cyber security, and emergency management programs throughout DOE by:

- Fostering an increased understanding of purposes, methods, and expectations
- Stimulating the exchange of knowledge and techniques for implementing protection programs
- Adding current field perspectives to appraisal activities.

Augmentees who participate in OA's field augmentation program acquire the following benefits:

- Detailed knowledge of OA's current methods, procedures, and areas of emphasis, which they can disseminate at their home sites. This knowledge can help home sites make program improvements and better understand OA's process, both of which can result in reduced levels of apprehension, increased cooperation, and smoother inspections at the home site.

- Participatory experience in planning, conducting, and reporting large-scale inspections. This experience can help strengthen survey and/or self-assessment programs at the home site.
- A detailed look at how other sites handle various protection challenges, possibly acquiring new ideas that can strengthen or economize protection programs at the home site.

As part of the OA augmentee program, OA-20 solicits augmentees who are highly qualified in cyber security policy and technical areas. Based on their technical qualifications and experience, augmentees may be assigned as inspection team members on the programmatic or technical review subteams. Participants involved in the technical review typically have an extensive background in network performance testing. Similarly, participants involved in the programmatic portion of the OA-20 inspections must be knowledgeable of DOE orders, policies, and initiatives. OA will provide the necessary orientation to assist new augmentees in using the inspection process protocols.

Augmentees must be volunteers who have been nominated and approved by the appropriate DOE Headquarters or field element manager and, if a contractor employee, by the appropriate company (employer) manager. OA will review each nominee's qualifications, will interview each nominee, and will make the final decision on each nominee's acceptance into the program.

Arrangement for a nominated augmentee to participate in an inspection will be arranged on a case-by-case basis, according to OA-20's needs, the availability and willingness of the augmentee, and the willingness of the augmentee's management to make him/her available during the period required. Augmentees will not be used on inspections that would involve a conflict of interest. Federal employees will not be used at their own sites or at sites where they or their organization have programmatic or supervisory responsibilities. Contractor employees will not be used at their own sites or at sites where their employer has

Planning

significant business connections. OA will pay travel expenses associated with augmentee participation in independent oversight appraisal

activities. Home organizations/employers must pay each augmentee's salary.

Section 4

CONDUCT

Contents

Introduction.....	17
Goal.....	17
Performance Testing.....	17
Programmatic Review.....	18
Communication and Feedback.....	18

Introduction

To gain insight into a site’s cyber security program for classified and unclassified information systems, and to understand interdependencies with other site activities, OA-20 uses a “bottom-up” approach to program assessment. As a first step, cyber security appraisals typically begin with extensive internal and external network performance testing that might include an initial site visit several weeks prior to the programmatic review (i.e., during the planning visit). Performance testing, including attempts to penetrate the site’s network, is also conducted remotely over the Internet from OA-20’s cyber security laboratories. OA-20 may also conduct tabletop reviews of computer systems excluded from performance testing, firewall rules, and intrusion detection systems to fully assess the protection provided by the network. As more fully discussed in Section 4.1, OA-20 will review any site request and site justification for exclusion of certain critical safety or operational systems from testing as part of the process of developing a performance test agreement.

During the conduct phase of the inspection, OA-20 finishes any remaining performance testing and performs a programmatic review to evaluate essential underlying management processes. This phase includes intense and varied activities such as interviews, walkthroughs, tabletop reviews, and data analysis that are customized to accurately assess the site’s ability to protect its classified and

unclassified networks. It is during this stage that OA-20 normally reaches assessment conclusions based on analysis of data; develops a draft report; and validates information with site personnel.

Goal

OA’s goal is to collect sufficient information as to the performance, direction, and sustainability of classified and unclassified cyber security programs during the conduct of an inspection, thus allowing a reasonable judgment of protection effectiveness.

Performance Testing

OA-20’s approach to performance testing activities is described in Appendix A. Performance testing is a key element of OA-20 cyber security appraisals since it provides tangible feedback on the current effectiveness of a site’s cyber security protection posture. While performance testing provides an indication of the current effectiveness of cyber security protection measures, it does not by itself allow for valid conclusions on the direction or sustainability of the program. This is assessed by conducting a programmatic review to evaluate essential management processes that form the foundation for the cyber security program. Performance testing results are used as a primary input for the programmatic review to identify specific weaknesses (symptoms) so that underlying causes or root causes of systemic problems can also be identified. It is the

Conduct

combination of extensive performance testing and a review of essential program elements that allows OA-20 to fully and effectively assess unclassified and classified cyber security programs.

Sites must ensure that DOE's Banner and Warning Policy has been implemented, thus informing network computer users that they have, as a result of use, granted consent to monitoring and by extension, OA-20 performance testing. Any misuse of computer systems detected during performance testing is reported immediately to site management. If criminal activity is suspected, OA-20 reports this information to the Office of the Inspector General (IG) for investigation and resolution. OA-20 does not investigate alleged criminal activity or misconduct. The site is responsible for reporting computer security incidents to program officials, CIAC, and other organizations, as appropriate. OA-20 is responsible for coordinating performance testing activities with CIAC. Performance testing procedures specific to OA-20 are contained in an internal Technical Standard Operating Procedure.

Programmatic Review

OA-20 programmatic reviews are conducted in a manner consistent with the guiding principles and core functions of ISSM/DCSM as described in DOE Policy 470.1 and DOE Policy 205.1 to assess the effectiveness of cyber security programs. Inspectors do not use a checklist to perform programmatic reviews; rather, they use the framework contained in Appendix B to help focus appraisal activities and to ensure that important elements are covered. The framework is structured around program direction and program implementation areas. Program direction considers both DOE line management and contractor roles and responsibilities in fulfilling ISSM/DCSM guiding principles. Program implementation evaluates program effectiveness in terms of the five core functions of ISSM/DCSM.

Through interviews, document reviews, and performance testing, the site-specific details of

each evaluation element are understood. Inspectors analyze these details and assess how the components are integrated to maintain an effective cyber security posture. The program review also encompasses extensive communication with site management and staff to ensure that facts and issues are accurately characterized. Elements of each component that inspectors review are discussed below. These elements are not intended to be prescriptive; rather, they illustrate the attributes of an effective cyber security program.

During program reviews, OA-20 evaluates the effectiveness of DOE cyber security policy and provides feedback to DOE's Office of the Chief Information Officer. In some cases, policy findings may be included in a site evaluation report. OA-20 also evaluates DOE program office and operations office performance as it relates to implementation of the cyber security program at the site.

Communication and Feedback

OA-20's objective throughout each appraisal activity is to ensure that a thorough and accurate assessment of a site's cyber security program(s) is conducted and that site personnel gain maximum benefit from the experience. To accomplish this, OA-20 personnel, site managers, and site cyber security staff must all communicate extensively. During both performance testing and programmatic reviews, OA-20 personnel provide routine feedback to the site on the progress of the inspection, keeping site personnel informed of any potential concern associated with the review. The site being inspected has an opportunity and responsibility to provide feedback to OA-20 personnel when concerns over factual accuracy exist. The site should provide additional data and identify site personnel who can help OA-20 personnel clarify any factual accuracy misunderstanding. The following activities are integrated into the OA-20 appraisal process to ensure that the inspection team and site managers and staff have an opportunity to effectively communicate:

- During remote performance testing, OA-20 technical personnel are in contact with site personnel routinely to discuss the status of testing and any issues.
- When conducting onsite programmatic review activities, the OA-20 inspection team will schedule a daily informal validation meeting with site cyber security staff to provide feedback on the progress of data collection, areas requiring further review, and issues of potential concern, if any.
- Also on a daily basis, a meeting is held between the Inspection Team Chief (or Team Leader/Topic Team Leader for an OA-20 only appraisal) and appropriate site managers to provide a management perspective on the progress of the programmatic review and performance testing.
- Once the inspection team completes scheduled data collection activities, a summary validation is held with site personnel to verbally brief the results of the appraisal and conclusions based on analysis of information.
- For onsite inspections, OA provides an initial draft inspection report to the site for review and comment prior to departing the site. For external network security assessments, the draft report is transmitted to the site for review and a conference call is set up to discuss factual accuracy. OA-20

team members consider comments from the site and make appropriate revisions to draft inspection reports.

- A closeout briefing is provided to key site managers at the conclusion of an inspection. The Inspection Team Chief, OA-20 Director, or Team Leader/Topic Team Leader orally presents the results of the appraisal to the site manager, highlighting program strengths, areas for improvement, and ratings for the site's classified and unclassified cyber security programs.
- OA-20 provides a final draft report that incorporates the changes from the initial review, and the site is provided another opportunity to provide factual accuracy comments on the report.

Periodically, sites ask for feedback on their approach to implement cyber security measures or products to use. As part of its effort to help DOE sites, OA-20 is open to conducting a dialogue on technical issues. As an independent oversight organization, OA-20 does not direct a site to take any specific action, use any specific cyber security tools, or adopt any specific technical solutions. Rather, OA-20 will engage in technical dialogue to provide feedback on the pros and cons of specific applications, approaches, and implementation. Selection of applications, approaches, and implementation is a line management responsibility.

This page intentionally left blank.

Section 5

CLOSURE

Contents

Introduction.....	21
Goal.....	21
Analysis of Results	21
Findings	22
Explanation of Rating System	22
Report Preparation	22
Quality Review Board	22
Briefings.....	22
Process Improvements	23
Documentation of Appraisal Activities	23

Introduction

The closure phase of an inspection typically occurs after data collection (document reviews, interviews, and performance testing) is essentially complete. OA-20 inspectors closely follow the process described in the OA Appraisal Process Protocols.

Goal

The main goal of this phase is to thoroughly analyze all available data and draw valid conclusions in order to prepare an appraisal report, assign ratings as appropriate, and inform site management of results.

Analysis of Results

While analysis is an ongoing process during all phases of an appraisal, it culminates during the closure phase. Analysis involves the critical review of all available information from the appraisal to identify specific strengths and weaknesses of a cyber security program as well as underlying root causes for that condition. The goal of analysis is to have logical, supportable conclusions that portray a fair picture of how well a cyber security program functions to

protect classified and unclassified DOE information technology resources. All team members work closely during this phase to ensure that all information and points of view are considered.

Weaknesses are analyzed both individually and collectively; they are balanced against strengths and mitigating factors to estimate their overall impact on performance (i.e., protection levels). This analysis leads to the identification of potential findings that document specific weaknesses. Factors that are considered during analysis of weaknesses include:

- The importance or significance of the weakness
- Whether the weakness is isolated or systemic
- Line management’s understanding of the weakness and actions taken to address the risk
- Mitigating factors, such as the effectiveness of other program elements that might compensate for the weakness and justify risk acceptance
- The actual or potential effect on mission performance or accomplishment
- Relevant DOE policy.

Findings

Findings are used to document significant weaknesses identified during appraisal activities associated with protection of information technology resources or essential underlying management processes that support the program. Findings are linked to appropriate national standards, public laws, executive orders, and DOE directives with which DOE cyber security protective programs must comply. Findings may be based on the most fundamental requirement to provide adequate protection to cyber systems or more specific implementation requirements. The Team Leader/Topic Team Leader is responsible for recommending the findings that should be assigned to a site's cyber security program as the result of an inspection.

Explanation of Rating System

The analysis of results leads to the assignment of ratings — Satisfactory, Marginal, or Unsatisfactory. The criteria for assigning ratings are stated in the OA Appraisal Process Protocols. Inspectors consider all facts and results from performance testing and the programmatic review when considering a rating. It should be noted that OA-20 performance testing provides a “snapshot in time.” A network's protection posture can change rapidly based on hardware or software changes or as new exploitation techniques are discovered; therefore, a rating of satisfactory should not promote complacency.

Report Preparation

A report is issued to formally document the results of appraisal activities and is intended for dissemination to the Secretary, appropriate DOE managers at Headquarters and in the field, and site contractors. While reports may vary in format, report preparation activities share a common process:

- The team prepares the initial draft report consistent with the data that have been collected and information that has been validated during the “conduct phase” of the appraisal.

- An OA Quality Review Board reviews the draft report to ensure that it is readable, logical, and contains adequate, balanced information to support the conclusions and ratings.
- The Director of OA approves any draft reports prior to providing it to the site for review.
- DOE and contractor personnel are given the opportunity to review draft reports for factual accuracy. The site is provided a relatively short time (normally less than a day) to review the initial draft report and provide informal factual accuracy comments. There is a turnaround time of ten working days for formal factual accuracy comments from the site associated with the final draft report. OA-20 team members review all factual accuracy comments, and changes are made to the report as appropriate. Factual accuracy reviews are not intended to allow reviewers to eliminate conclusions, findings, or ratings that the site or managers view as unfavorable. Follow-on interviews or documentation reviews may be required to validate information provided by the site as a consequence of factual accuracy reviews.

Quality Review Board

The Quality Review Board is established as an internal process that provides for a fresh set of eyes to review draft reports from a management perspective prior to review by the Director of OA and then the site. The Quality Review Board provides feedback on the readability of the report, whether or not the analysis and conclusions are appropriately supported, and whether the standards applied are consistent with other OA appraisal activities. The Quality Review Board is typically chaired by the Deputy Director of OA and includes the OA-20 Director, and other senior personnel as directed. For joint appraisals with OA-10, the OA-10 Director would also be included.

Briefings

Part of the closure process is briefing line management on the results and conclusions of

the appraisal activity. Prior to leaving the site, OA provides an exit briefing to summarize the results of the appraisal activity to key DOE field and contractor line managers. For external network security assessments that are conducted remotely, the OA-20 Director (or Deputy) and Team Leader/Topic Team Leader will travel to the site after receiving factual accuracy feedback on the initial draft report to brief management on the results.

Process Improvements

OA-20 believes in the concept of continuous improvement in order to make cyber security appraisals more effective and of value to DOE sites, departmental managers, and other stakeholders. Consistent with that tenet, OA-20 team members participate in a lessons-learned roundtable during the closure phase of each appraisal. The Team Leader/Topic Team Leader is responsible for soliciting feedback from each team member and making recommendations to the OA-20 Director on process improvements.

OA also solicits feedback from DOE field and contractor line managers to ensure that the appraisal process provides value to site personnel. OA welcomes any feedback on how appraisal processes can be improved to make them more effective.

Documentation of Appraisal Activities

In conducting the inspection, OA-20 inspectors collect a large volume of data and information through performance testing, document reviews, and interviews. While OA-20's appraisal processes are designed to assure the factual accuracy of information presented in assessment reports, information is retained to provide supporting evidence. This is necessary considering that one aspect of OA-20's mission is to conduct the annual evaluation of DOE classified information technology systems and to provide input to the annual evaluation of DOE unclassified information technology systems as required by the Government Information Security Reform Act. Part of this process is undergoing an audit by the IG to validate OA-20 appraisals. Retention of key documentation is

necessary to provide IG auditors the information necessary to independently reach the same conclusions as contained in OA-20 appraisal reports.

Each member of an OA-20 appraisal team has a role in documenting assessment activities. This includes:

- Developing planning documents
- Documenting interviews and other site assessment activities
- Retaining important site documents that were reviewed
- Recording performance testing results
- Reflecting assessment conclusions in appraisal reports.

The OA-20 Team Leader/Topic Team Leader is responsible for ensuring that key appraisal information is captured and retained. As a rule, OA-20 will not retain large volumes of classified information in support of documenting appraisal activities. While classified interview sheets will be retained under appropriate security controls, classified documents reviewed will not normally be kept. OA-20 will also retain any classified performance testing results following all security requirements. The OA-20 Team Leader/Topic Team Leader is responsible for reviewing all information that was used as part of the appraisal and was relevant to the conclusions developed, and for making a determination as to whether it should be retained or not. To prevent managing large quantities of paper documents, a high-speed scanner will be used whenever possible to convert information to electronic format so it can easily be stored on compact discs. All appraisal documentation that is retained will be for internal use only, except as authorized by the OA-20 Director in support of IG audits and other valid reasons. Specific information that should be retained from an inspection includes:

- Inspection plan
- Performance test agreement
- Document request list
- Schedules of interviews

Closure

- Internal and external network vulnerability scanning results (for classified and unclassified networks)
- Phone sweep results
- Details associated with any exploits that were conducted during performance testing
- Network architecture diagrams and other relevant technical data
- Daily internal team reports
- Interview notes
- Key documents that were reviewed as part of the appraisal (e.g., security plans, risk assessments, self-assessments, procedures)
- Issue forms

- Initial and final drafts of reports
- Any other information from the appraisal determined to be worthwhile.

To help in the organization of information that is retained from an appraisal, the OA-20 Team Leader/Topic Team Leader will develop a summary list of interviewees and key documents reviewed to go along with information described above. For those cases where the documents are not retained or stored in another location due to security considerations, the summary lists will make note of this. Blank summary lists that will be used are contained in Appendix E.

Section 6

FOLLOW-UP

Contents

Introduction.....	25
Goal.....	25
Headquarters Briefings	25
Final Reports.....	25
Corrective Action Plans	26
Corrective Actions and Follow-Up.....	26

Introduction

The OA Appraisal Process Protocol and DOE Order 470.2A describe in detail the requirements associated with providing Headquarters briefings, finalizing the inspection report, and developing initial, interim, and final corrective action plans in response to inspection findings. OA-20 adheres to the guidelines and time frames established in these documents. Sites should also refer to these documents for expectations on providing factual accuracy comments on the final draft report and submitting corrective action plans in response to identified findings.

Goal

The primary goal of the follow-up phase is to finalize and publish the appraisal report, brief the results of the assessment to appropriate personnel, and establish an adequate corrective action plan.

Headquarters Briefings

After leaving the site, OA will routinely provide briefings on appraisal activities to appropriate Headquarters officials with an interest and role in the program. This group may include the Office of the Secretary, Under Secretaries, Program Secretarial Officers, Program Office Personnel, the Office of the Chief Information

Officer, and the Office of Counterintelligence. A strategy for conducting Headquarters briefings will be developed after each appraisal.

OA may be requested to provide briefings to external stakeholders such as Congressional Committees, Members of Congress, and Congressional Staff Members. These briefings will be conducted on a case-by-case basis as appropriate after being coordinated through the Congressional Liaison Office. Briefings to external stakeholders will not normally take place until after a final report is issued.

Final Reports

OA-20 follows the requirements established by DOE Order 470.2A and guidance in the OA Appraisal Process Guide on formal comments associated with the factual accuracy of final draft appraisal reports. OA-20 will fully consider each comment received, review documentation, and conduct additional discussions with site personnel to determine an appropriate disposition. Comments may be incorporated, partially incorporated, or dismissed based on the facts of the situation. OA-20 personnel will communicate the disposition of comments to site personnel. After the resolution of final comments, OA-20 will publish the final report in accordance with OA procedures.

Corrective Action Plans

Sites should follow the requirements established by DOE Order 470.2A and guidance in the OA Appraisal Process Protocols in developing corrective action plans in response to findings identified in OA-20 appraisal reports. These plans should assign responsibility to an individual and contain interim and final milestones as appropriate. Corrective action plans should address the root cause of the finding and compensatory measures that should be implemented if a solution cannot be implemented in a short time. Key decision points should be identified, as appropriate.

Corrective Actions and Follow-up

In accordance with Secretarial guidance, program offices and DOE sites are responsible for entering findings and corrective actions into a Corrective Action Tracking System, updating the corrective action status, and closing findings. OA will ensure that cyber security findings are entered in the Safeguards and Security Information Management System (SSIMS) for those sites with access to the system. For any sites that do not have SSIMS access and have unclassified program findings, OA will track these findings separately. OA-20 will monitor the progress of corrective actions through the conduct of follow-up reviews and subsequent appraisals.

APPENDIX A

CYBER SECURITY PERFORMANCE TESTING APPROACH

CYBER SECURITY PERFORMANCE TESTING APPROACH

A.1 Purpose

Performance testing can be divided into two main categories—external and internal. External testing assesses the site’s effectiveness in addressing threats from the Internet, (e.g., hackers, foreign intelligence agencies, and economic competitors). Internal performance testing addresses threats from authorized users (e.g., disgruntled employees, visiting researchers, and foreign nationals) seeking access to information or computer services for which they are not authorized. Internal testing assesses the site’s ability to keep authorized users (both classified and unclassified) from migrating beyond predetermined “need-to-know” boundaries.

Performance testing is conducted in four phases during which various tools and techniques are applied to identify vulnerabilities associated with the site’s computer systems, and attempt penetrations of networked computers to assess the significance of these vulnerabilities. These four phases—information gathering, scanning, penetration, and reporting—apply to both external and internal performance testing. Testing includes employing techniques, such as footprinting, scanning, enumeration (making active connections to systems and directed queries), gaining access to systems, and escalating privileges, that hackers use in attempting to penetrate and control a network. The Office of Independent Oversight and Performance Assurance Office of Cyber Security and Special Reviews (OA-20) performance testing, discussed below, results in a rigorous evaluation of the site's cyber security implementation. These results are provided to the site, which can use this information to further strengthen their cyber security.

A.2 Information Gathering

OA-20 obtains much of the required information regarding the site’s network profile, such as Internet Protocol (IP) address ranges, telephone number ranges, and other general network topology, through public information sources (e.g., Internet registration services, Web pages, and telephone directories). OA-20 then obtains more detailed information about the site’s network architecture through domain name server (DNS) queries, ping sweeps, port scans, and connection route tracing. OA-20 might also engage in covert attempts to gather information from users and administrators that could assist in gaining access to network resources. Any such activities will be coordinated with selected site personnel. Once this general network information is compiled and analyzed, OA-20 identifies individual system vulnerabilities.

A.3 Vulnerability Scanning

During this phase, OA-20 attempts to associate operating systems and applications with identified computers on the network. Depending upon network architecture, they might use automated tools (e.g., nmap, queso) and/or manual techniques (e.g., telnet, FTP (File Transfer Protocol), or sendmail login banners). From this information, OA-20 develops a list of probable vulnerabilities associated with each potential target system. Also, at this point, OA-20 develops or compiles automated scripts to attempt exploitation of vulnerabilities.

OA-20 also uses an automated modem search tool to identify network vulnerabilities via a phone modem. This tool dials all of the site's phone numbers to identify which, if any, of the telephone numbers are used for computer modems in “auto-answer” mode. This mode could allow a hacker to circumvent the external network security perimeter and gain unauthorized access to computer systems and electronically stored information.

A.4 Network Penetration Testing

Using information from network mapping and automated scanning, OA-20 attempts to access systems behind the Internet firewall(s) to evaluate the effectiveness of barriers intended to protect against external threats. OA-20 also evaluates the effectiveness of barriers (host-level security features) that protect against internal threats. Vulnerabilities that may be exploited include, but are not limited to: buffer overflows, application or system configuration problems, modems, routing issues, DNS attacks, address spoofing, share access, and exploitation of inherent system trust relationships. Potential vulnerabilities are systematically tested in the order of penetration and detection probability as determined by the OA-20 penetration testing team. The strength of captured password files will be tested using password-cracking tools. Individual user account passwords might also be tested using dictionary-based, automated login scripts. If an account is compromised, OA-20 attempts to gain the privileges of a “super user,” root, or administrator.

Since the goal of OA-20 testing is to determine the extent of vulnerabilities, and not simply to penetrate a single site system, OA-20 can use information discovered on one system to gain access to additional systems that may be “trusted” by the compromised system. Additionally, OA-20 may exploit host-level vulnerabilities to elevate privileges within the compromised system to install “sniffers” or other utilities. OA-20 inserts a small text file at the highest-level directory of each compromised system. If OA-20 cannot gain sufficient privilege to write to the system, a file will be copied from the system. In either case, OA-20 may copy additional files during testing if necessary to determine the sensitivity of the information contained on the system.

A.5 Reporting

OA-20 maintains detailed records of all attempts to exploit vulnerabilities and activities conducted during performance testing. The results of OA-20 scans and penetration testing are provided to established points of contact so the site can take corrective actions to address identified vulnerabilities. OA-20's records provide enough detail to aid the site in removing added programs and files, identifying systems with compromised password files, and returning the systems to their original configurations; therefore, no systems are left in a compromised condition.

OA-20's external network security assessment closely follows the performance testing protocols discussed above, except all testing is initiated from outside the network perimeter. Specifically, the external network security assessment includes:

- Conducting vulnerability scans of computer systems exposed to the Internet
- Evaluating the effectiveness of network firewalls
- Reviewing intrusion detection strategies and effectiveness
- Conducting modem phone sweeps (e.g., checking the security of alternative pathways into the network).

APPENDIX B

CYBER SECURITY PROGRAM EVALUATION FRAMEWORK

CYBER SECURITY PROGRAM EVALUATION FRAMEWORK

Cyber Security Program Direction

U.S. Department of Energy (DOE) Line Management Responsibilities

DOE line management is responsible for:

- Establishing clear cyber security roles, responsibilities, authorities, delegations and interfaces between DOE Headquarters, field organizations, and the site including coordination of line management direction from multiple program offices.
- Establishing and communicating, through contracts and other mechanisms, expectations for cyber security performance for DOE, contractor, and other organizations. DOE line management has established and tracks clearly defined, meaningful, and challenging performance measures that are tied to contract incentives.
- Ensuring that DOE Headquarters and field office line management is involved in, cognizant of, and supportive of priorities associated with cyber security.
- Providing timely and sufficient guidance on expectations for implementation of cyber security requirements, standards, and DOE initiatives.
- Incorporating cyber security requirements into binding agreements, such as a contract, to ensure timely implementation by contractors, subcontractors, privatization contractors, and lessees utilizing DOE information technology resources.
- Reviewing and approving security plans for classified systems and computer security program plans for unclassified systems to ensure protection strategies are appropriate and effective. DOE line management has an understanding of and accepts the residual risk for operating classified and unclassified information technology systems.
- Establishing effective, performance-based processes for monitoring and assessing contractor cyber security performance, providing feedback, and holding the contractor accountable for effective performance and correction of deficiencies. Ensuring that surveys are conducted at required intervals and are effective in evaluating classified and unclassified cyber security programs. Privatization contractors and lessees are also assessed if they are operating or utilizing DOE information technology systems.
- Holding contractors and personnel accountable for the effectiveness of cyber security performance.

Site Line Management Responsibilities

The site line management is responsible for:

- Ensuring that senior line management demonstrates a commitment to cyber security and promoting its understanding, acceptance, and timely implementation. Additionally, initiatives to improve classified and unclassified cyber security programs are championed, as appropriate.
- Establishing and communicating a set of policies and performance expectations consistent with DOE's *Integrated Safeguards and Security Management (ISSM) Policy*, DOE Policy 470.1, and the *Departmental Cyber Security Management (DCSM) Policy*, DOE Policy 205.1. Ensuring that challenging cyber security program goals are established and tracked to accomplishment through performance metrics. Organizations and individuals are held accountable for cyber security performance.
- Implementing and integrating both horizontal and vertical integration of cyber security throughout organization functions at all organizational levels. Assuring that managers and supervisors at all

levels accept, actively promote, and set an appropriate example for the integration of cyber security into site activities.

- Providing roles, responsibilities, and authorities for cyber security that are clearly defined, documented and understood by organizations and individuals (including line managers, cyber security staff, and computer users) at every level in the organization.
- Implementing processes to ensure that cyber security responsibilities and authorities flow down consistently from senior management to each person utilizing or interfacing with site information technology resources (including employees, subcontractors, temporary employees, visiting researchers, vendor representatives, lessees, etc.).
- Clearly defining functional relationships and responsibilities among all organizational entities that share information technology resources or are incorporated within the site's trusted network structure.
- Holding accountable all DOE and contractor personnel, including managers, supervisors, users, and administrators, for cyber security performance through a combination of performance expectations, incentives, and negative consequences for poor performance.
- Utilizing risk-based decision-making processes to resolve disputes, establish priorities, and balance operational needs against cyber security requirements.
- Establishing an effective, consistent, and risk-based decision-making process for appropriately funding cyber security, including providing resources for addressing identified issues, deficiencies, and commitments.
- Involving system administrators, users, project managers, and stakeholders in the prioritization and allocation of resources to maintain an appropriate balance between operational needs and cyber security requirements.
- Establishing effective management systems that link cyber security issues, commitments, and deficiencies to business mechanisms associated with planning, prioritizing, and budgeting.

Cyber Security Program Implementation

Define the Scope of Work

To define the scope of work, the site is responsible for:

- Assuring the effective integration of cyber security into all applicable business processes. Ensuring that cyber security needs are considered when defining new projects and/or work.
- Actively involving cyber security personnel, workers, program personnel, and stakeholders to ensure an appropriate balance between mission objectives and protection of DOE information technology resources.
- Providing formal processes that incorporate cyber security considerations over the life cycle of projects to achieve DOE expectations for security. Assuring that a well-defined work planning and control process is in place that embraces the core functions of ISSM/DCSM.
- Assuring that the site's hierarchy of work planning processes provides increasingly detailed descriptions of the work at successively lower tiers such that broad mission objectives are eventually translated into discrete tasks that address cyber security needs.
- Developing the level of detail and formality in a scope of work that is commensurate with the importance of the work, its complexity, and potential threats to information technology systems.
- Instituting an ISSM/DCSM system that provides for integration of cyber security into all work or projects involving DOE information technology systems.
- Establishing processes to assure the identification and minimization of threats to information technology resources associated with new work and projects. Assuring that the definition of the scope of work is an integrated and collaborative activity that considers cyber security and involves all appropriate organizational units.

- Assuring that effective management systems, processes, and controls are in place to assure that the implementation of ISSM/DCSM and the integration of cyber security into all work activities is a coordinated and collaborative effort.

Analyze the Risk

To analyze the risk, the site is responsible for:

- Continually assessing the threats, vulnerabilities, and risks associated with DOE information technology systems.
- Identifying information technology mission critical systems that require protection. Additionally, identifying the types and sensitivities of data on information technology systems in order to properly assess risks.
- Establishing mechanisms and processes to gather threat and vulnerability information to be considered during risk assessments.
- Establishing and implementing a disciplined, documented, methodical, and collaborative approach for ongoing cyber security risk assessments.
- Tailoring risk assessments and the extent of management review according to the type and sensitivity of information technology resources being protected and the significance of risk. Assuring risk assessment processes balance the need for confidentiality, integrity, and availability of information systems with operational needs.
- Establishing effective management controls and processes to assure the involvement of appropriate information technology professionals, system administrators, and users in the risk assessment process.
- Establishing processes to assure that the shared risk between network segments or as a result of trust relationships is fully assessed.
- Assuring that when new cyber security threats and risks are identified, requirements are reassessed for adequacy.

Develop and Implement Security Measures

To develop and implement security measures, the site is responsible for:

- Establishing processes for identifying and tailoring protection strategies to address risks associated with operating DOE information management systems. Establishing controls that address both internal (e.g., malicious insider) and external (e.g., intruder) cyber security threats.
- Establishing effective risk mitigation strategies for DOE information technology systems over their life cycle to reduce or mitigate threats.
- Considering protection strategies in terms of near-term and long-term solutions and other factors (such as assigned mission, reliability, system performance, timeliness, life-cycle costs, and technical barriers). Applying a preferred hierarchy in identification of controls that considers engineered/technical solutions first, and administrative controls second.
- Identifying compensatory measures to address risks until time and resources are available to implement more optimal controls.
- Implementing an effective collaboration process for establishing cyber security controls that assures participation by personnel who understand the risks involved as well the work activity and information management systems involved.
- Implementing processes for managing cyber security requirements, including the translation of requirements and guidance into policies, programs, and procedures.
- Establishing requirements commensurate with the threat and risk to information technology systems (i.e., the cyber security requirements identification process is linked to the risk management process).

Ensuring that site policies, guidance, and procedures conform to Federal and DOE cyber security requirements.

- Appropriately incorporating cyber security requirements into the site’s Cyber Security Program Plan for unclassified systems and security plans for classified systems.
- Establishing additional procedures, as necessary, that tailor site requirements to specific situations and provide sufficient detail to implement cyber security requirements at the working level.
- Documenting and gaining line management acceptance of residual risk associated with the DOE information technology resources prior to operation. Assuring that additional cyber security controls are put in place if the level of residual risk is unacceptable to line management.
- Adequately documenting cyber security controls in cyber security program plans for unclassified systems and security plans for classified systems in a manner that assures technical accuracy, usability, and quality. Implementing effective management processes to assure that these plans are maintained current and accurate.
- Assuring that the site has processes in place to test, implement, manage, maintain, and revise cyber security controls as necessary to be effective.
- Properly analyzing significant changes in design, life cycle, operations, or conditions for their impact on the protection of information technology resources, and ensuring that cyber security controls are modified as appropriate.
- Fully defining the site’s network perimeter and establishing line management controls that provide adequate protection for information technology resources.
- Establishing controls to ensure that foreign nationals and other collaborators obtain approvals prior to being granted access to DOE information technology resources.
- Establishing processes to control user access to classified information stored electronically on information technology systems by establishing strong “need-to-know” controls. This includes establishing “need-to-know” boundaries within classified networks and administrative processes to control the number of users in “need-to-know” groups.
- Ensuring processes are in place to fully document trusted network relationships and assure that strict controls are in place to mitigate the introduction of vulnerabilities.
- Establishing stringent controls over downloading files from classified to unclassified systems.
- Establishing additional controls for classified laptop computers to mitigate the additional risk associated with the portability of these devices.
- Establishing controls over modems to prevent them from providing backdoors into the network and undermining protection strategies.
- Establishing communication mechanisms to ensure that managers, system administrators, and users remain aware of cyber security policies, procedures, and guidance applicable to their responsibilities.
- Determining and documenting the appropriate levels of cyber security staffing, education, experience, and training for technical personnel. Using needs analysis and job/task analysis to support staffing levels and training requirements.
- Identifying critical cyber security skills that are needed to implement cyber security measures and developing and implementing short-term and long-term strategies for recruiting and retaining competent personnel.
- Assuring that effective processes are in place so that all managers and users are adequately trained on cyber security risks, policies, and requirements prior to being given access to DOE information technology resources. Conducting annual training to ensure that all managers, users, and technical personnel maintain this understanding.

Perform Work Within Measures and Controls

To perform work within measures and controls, the site is responsible for:

- Assuring that personnel are qualified and knowledgeable of their responsibilities as they relate to cyber security controls and work performance.
- Establishing adequate cyber security staffing levels necessary to maintain an effective program.
- Commensurate with their responsibilities, assuring that site information technology personnel demonstrate a high degree of competence in implementing their cyber security responsibilities for DOE information technology resources. Assuring that these personnel also demonstrate an in-depth understanding of cyber security threats, requirements, and protection strategies.
- Ensuring that mechanisms are in place so that only qualified and competent personnel are assigned to technical work activities associated with securing and maintaining DOE information technology resources.
- Defining responsibilities and authorities for verifying readiness to operate information technology resources, including the appropriate level of review and approval for accrediting classified systems. Ensuring that formality and rigor used to confirm readiness is based on the level of threat and risk.
- Establishing a process to confirm that the cyber security risk assessment that was performed and the controls that have been put in place are adequate to provide a level of protection to information technology systems commensurate with the level of threat and risk.
- Empowering line management individuals and encouraging their participation to protect information located on information systems.
- Assuring that processes are in place to ensure that personnel are qualified and trained to implement controls in accordance with established cyber security requirements, policies, and procedures.
- Establishing and agreeing upon controls and requirements for operating information technology resources prior to operations being initiated. Assuring that DOE has either directly authorized (where appropriate) or delegated approval authority, within clearly defined limits, to the contractor for cyber security program plans for unclassified systems and security plans for classified systems.
- Establishing processes in place to ensure that all network and standalone system operations are conducted within established controls and follow requirements. Cyber security procedures are followed and mechanisms are in place to hold managers, system administrators, and users accountable for performing work within controls.
- Establishing processes for withdrawing accreditation/operations authorization for information technology systems deemed to be inadequately secured or protected.
- Assuring that site personnel adhere to cyber security controls and follow established procedures as a means to ensure adequate protection of DOE information technology resources.
- Assuring that managers, system administrators, and users appropriately implement the requirements for password protection and access controls in order to protect information technology resources from unauthorized use.
- Assuring that DOE's Banner and Warning Policy is appropriately implemented on all DOE information technology resources.
- Assuring that site perimeter protection controls are effectively implemented, including the management of firewalls, filter routers, and screened subnets to provide appropriate protection to network resources.
- Assuring that processes are in place to evaluate "need-to-know" requirements for individual managers and users. Additionally, line management ensures effective implementation of "need-to-know" boundaries within networks to protect sensitive or classified information.
- Establishing that configuration management processes to control hardware and software modifications associated with site information technology systems are in order to prevent existing controls from being undermined through the introduction of vulnerabilities.

- Establishing processes for monitoring and auditing information technology systems to ensure that configurations remain secure and unauthorized activities are prevented.
- Based on the level of threat and risk, assuring that intrusion detection systems provide an appropriate level of monitoring and coverage for detecting malicious activity on networked resources.
- Establishing processes for reporting/responding to computer security incidents.
- Assuring that “need-to-know” controls for classified systems are effectively implemented and result in only those personnel with a true “need-to-know” being granted access to classified information stored electronically on information technology systems.
- Establishing ongoing processes for identifying and correcting network vulnerabilities to ensure that cyber security controls remain effective and networked systems are adequately protected. Assuring line management also identifies and corrects vulnerabilities associated with modems.
- Assuring that modem controls are effectively implemented to protect against unauthorized access to the network.
- Assuring that the Cyber Security Program Plan for unclassified systems and security plans for classified systems are fully implemented and effective in protecting information technology resources.
- Assuring that processes are in place for sanitizing computers prior to their disposal.

Provide Feedback and Continuous Improvement

To provide feedback and continuous improvement, the site is responsible for:

- Demonstrating a commitment to achieving continuous improvement in cyber security.
- Establishing a process for planning and conducting self-assessments, management assessments, and performance-based testing. Assuring contractor assessment activities are effective in identifying cyber security issues and weaknesses associated with current performance.
- Establishing mechanisms for obtaining feedback from managers, systems administrators, and users as a means of identifying potential improvements to cyber security. Assuring managers, system administrators, and users participate in self-assessment activities.
- Communicating upward the results of assessments and other performance information, from line management to senior management, to enable informed determinations as to the effectiveness of ISSM/DCSM and cyber security performance. Assuring results are also communicated downward with expectations for future performance.
- Establishing mechanisms to identify cyber security lessons learned from multiple sources. Assuring processes have been established to communicate these lessons learned to appropriate personnel through training, bulletins, and other similar avenues.
- Implementing processes to develop and track performance measures to monitor cyber security program effectiveness. Assuring performance measures are linked to performance objectives and expectations established by line management.
- Being cooperative with and responsive to DOE and other external oversight activities, as part of its commitment to continuing cyber security program improvements.
- Responding to identified deficiencies, adverse trends in performance measures, generic issues, recurring events, or other indicators by implementing meaningful corrective actions. This includes improvements to management systems and processes.
- Assigning responsibility for actions, identifying milestones, and committing resources when establishing cyber security corrective action plans.
- Analyzing cyber security incidents and deficiencies (identified by any source) to determine root causes, systemic issues, and measures necessary to prevent recurrence.

- Establishing processes for tracking cyber security issues and associated corrective actions to completion. Assuring that priority for closure of issues is risk-based. Closure of deficiencies and corrective actions is based on objective, technically sound and verified evidence.
- Providing periodic status updates to line management on the status of identified cyber security deficiencies and corrective actions and holding organizations and individuals accountable for timely completion of actions.
- Establishing and implementing an effective process for monitoring and assuring the continuing quality of training programs.

This page intentionally left blank.

APPENDIX C
REFERENCE DOCUMENTS

REFERENCE DOCUMENTS

1. DOE Order 200.1, *Information Management*, dated 9-30-96, assigns responsibilities and authorities and prescribes policies, procedures, standards, and guidelines for the orderly disposition of the records of the U.S. Department of Energy (DOE).
2. DOE Manual 200.1-1, *Telecommunications Security Manual*, dated 3-15-97, 1360.1A, provides general guidance for the use, review, coordination, and provision of telecommunications services for the DOE.
3. DOE Policy 470.1, *Integrated Safeguards And Security Management (ISSM) Policy*, dated 5-8-01, establishes a formal, organized process for planning, performing, assessing, and improving the secure conduct of work in accordance with risk-based protection strategies.
4. DOE Order 471.2A, *Information Security Program*, dated 3-27-97, and its associated manual, DOE Manual 471.2-2, establishes policy and provides guidance for the DOE concerning the protection, control, and management of DOE classified and sensitive information.
5. DOE Manual 475.1-1, *Identifying Classified Information*, dated 5-8-98, provides guidance for the management of the DOE classification system.
6. DOE Policy 205.1, *Departmental Cyber Security Management Policy*, dated 5-8-01, explains the DOE ISSM policy within the cyber security realm.
7. DOE Notice 205.1, *Unclassified Cyber Security Program*, dated 7-26-99, establishes policy for safeguarding DOE data processing systems and, in particular, DOE sensitive unclassified information.
8. DOE Notice 205.2, *Foreign National Access To DOE Cyber Systems*, dated 11-1-99, establishes requirements for foreign national access to DOE information systems.
9. DOE Notice 205.3, *Password Generation, Protection, and Use*, dated 11-23-99, establishes minimum requirements for the generation, protection, and use of passwords to support authentication when accessing classified and unclassified DOE information systems.
10. DOE Order 5636.3A, *Technical Surveillance Countermeasures Program*, dated 2-3-88, establishes the DOE Technical Surveillance Countermeasures Program.
11. DOE *Statement of Generic Threat to Information Systems*, dated 2/01, identifies generic threats to DOE information resources.
12. OMB Circular A-130, "Management of Federal Information Resources," dated 7-15-94, as amended, promulgates policy and responsibilities for the development, implementation, and management of Federal information resources.
13. Policy Letter, "Use of Warning Banners on Departmental Computer Systems," from Chief Information Officer to Heads of Departmental Elements, dated 6-17-99, requires the use of computer screen warning banners that notify all computer users, prior to gaining access to system resources, that system usage is subject to monitoring and disclosure by appropriate site, DOE, or law enforcement personnel.
14. Policy Letter, "Enhanced Protection Measures," from Secretary of Energy to DOE Operations Offices, dated 6-19-00, requires encryption of select high-density media containing classified information and control of classified documents.
15. Presidential Decision Directive 63, *Protecting America's Critical Infrastructures*.
16. Public Law 100-235, "Computer Security Act of 1987," dated 6-11-87, provides for a computer standards program within the National Institute of Standards and Technology to provide for government-wide security and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes.
17. Public Law 83-703, Atomic Energy Act of 1954, as amended, provides the policy to control the dissemination and declassification of Restricted Data in such a manner as to assure the common defense and security.

This page intentionally left blank.

APPENDIX D

SAMPLE INDEPENDENT OVERSIGHT CYBER SECURITY PERFORMANCE TEST AGREEMENT

**SAMPLE INDEPENDENT OVERSIGHT CYBER SECURITY
PERFORMANCE TEST AGREEMENT**

SITE: ANY DOE SITE

DATES: From: Day/Month/Year To: Day/Month/Year

OBJECTIVE:

To provide an assessment of the internal and external security profile of the site's unclassified networked computer systems and a security profile of the site's classified computer systems. Testing is composed of the following primary elements:

1. Identifying network and dial-up vulnerabilities using various scanning techniques and through review of technical information
2. Attempting to exploit some identified vulnerabilities to determine whether weaknesses allow unauthorized access to sensitive information and escalation of privileges within the network
3. Reviewing firewall rules, border router access lists, intrusion detection architecture and system parameters, Private Branch Exchange (PBX) security architecture, and classified "need-to-know" boundaries.

SCENARIO:

Identification of Vulnerabilities

External Network Assessment

The first part of the Office of Cyber Security and Performance Assurance's (OA-20's) assessment will consist of an external network assessment. OA-20 will use its own computer resources from its off-site laboratory to conduct vulnerability scanning and penetration testing of the site's external unclassified computer networks. OA-20 will be allowed to scan the external segments of the network for vulnerabilities without being blocked.

External penetration testing will be conducted from remote computer systems to assess whether potential vulnerabilities of Internet barriers (e.g., firewalls) are exploitable from the Internet. During the external network testing, the site will maintain its normal network configuration while OA-20 attempts penetration over the Internet from its testing laboratory. Remote testing may include additional scanning to identify computer systems that have vulnerabilities or configuration anomalies that could allow unauthorized access from the Internet. No data files will be deleted. Additionally, all information obtained by OA-20 will be protected from unauthorized access in accordance with U.S. Department of Energy (DOE) orders and applicable Federal requirements. The site will not take any deliberate actions to block OA-20 testing activity except for automated processes already in place. Intrusion logs of any OA-20 events should be kept and later, during the assessment, OA-20 will review the effectiveness of the site's intrusion detection system.

OA-20 will use an automated modem search tool (i.e., war-dialer) to scan through the range of telephone numbers applicable to the site. War-dialing will be accomplished from the OA-20 offsite lab or by site owned war-dialing equipment. At the discretion of OA-20, recent site war-dialer records may be used to meet the requirement. The war-dialer tool will identify which, if any, of the telephone numbers are used

for computer modems in “auto-answer” mode. Modems identified through testing will be compared with the site's list of known modems.

Internal Network Assessment

The next part of the assessment includes an onsite visit by the OA-20 technical team to evaluate systems located behind the site firewall(s). OA-20 will use the same automated tools and techniques as those used for external network assessment.

To accomplish these internal tests, OA-20 will use some of its own computer resources and four computers provided by the site that reside on the site's sensitive unclassified network. OA-20 laptop systems will require access to both the unclassified network and the Internet. These systems are necessary because some assessment software is licensed for a specific system and cannot be moved to a site-provided computer system. It is imperative that three of the site-provided systems meet the following *minimum* specifications: Windows 2000, with the latest service pack, and the latest version of Internet Explorer (for unclassified network evaluation only). The fourth site-provided system will be a Linux system, preferably RedHat version 7.1. All systems need to be at least a Pentium III, 600MHz, with at least 512MB RAM, 10GB of hard disk space, and 17-inch monitors with adequate video support for a resolution of 1024 x 768. All systems need to be configured to allow OA-20 to have local-administrator privileges. They also need to be configured to allow sharing of file systems and resources, to include printers. These requirements must be met to support use of the automated tools, such as Internet System Scanner (ISS). In addition, OA-20 will need to have available a CD-RW drive to save scanning results to a CD-ROM for later analysis. One system should have a printer directly connected to the workstation or a printer that is accessible via the network. The location of the systems provided should be on the site's network backbone or on a network segment with a throughput of at least 100Mbs.

This part of the assessment phase will also include vulnerability scanning of the classified network. OA-20 will use an authorized site computer system already residing on the classified network. If the site has the latest version of ISS on a system set up for scanning, OA-20 will use this system. If ISS software is not on the system, OA-20 will provide the ISS software and the license key for the vulnerability scanning. The site will authorize the software to be installed on the classified network and will allow OA-20 or a site representative access on that system at the local-administrator level to conduct the scans. The system should meet the requirements listed above. OA-20 will need to review the classified network topology and review any filtering router configuration. OA-20 will review any technologies implemented for authentication, file, or database access, or any permissions in place that segregate or limit access to classified data. OA-20 will review the “need-to-know” boundaries if there is any technical implementation different from what was discussed above.

OA-20 will conduct a desktop review of the PBX that provides phone service to the site. The review will include such parameters as setup and configuration of the PBX, any security implementations on the PBX, the logs generated by the PBX, the maintenance procedures, and the permissions for users or administrators.

Exploitation of Identified Vulnerabilities

External Network Assessment

OA-20 will evaluate the effectiveness of barriers (i.e., host-level security features) that protect against external threats. Examples of vulnerabilities that may be exploited during penetration testing include, but are not limited to: buffer overflows, application or system misconfiguration problems, routing issues, DNS attacks, cracking of captured passwords, address spoofing, share access, and exploitation of inherent

system trust relationships. If a user account is compromised, that account will be tested for access permissions and attempts will be made to subvert systems into granting super user, root, or administrator access to the device. Any additional information discovered may be used to gain access to other systems or targets. Other attack tools or information gathering tools may be installed to further the penetration of targets, depending on need and applicable protocols. OA-20 will expeditiously (to the greatest extent possible) report vulnerabilities as they are discovered and validated so that systems will not be left vulnerable.

Internal Network Assessment

OA-20 will also assess the ability of an inside user to traverse the network and gain access to resources outside the boundaries of officially allocated privileges. In addition to internal vulnerability scanning, OA-20 will conduct internal penetration testing. Examples of vulnerabilities that may be exploited during penetration testing are similar to those described above. These include, but are not limited to: cracking of captured passwords, share access and exploitation of inherent system trust relationships, misconfiguration problems, deploying “sniffers” to capture passwords, keystroke loggers, trojans, and various computer forensic techniques that may reveal user and system login/account information.

Results

OA-20 will provide the results of scans and penetration testing to established points of contact at the site to facilitate corrective actions for identified vulnerabilities. OA-20 will also provide an adequate level of detail to facilitate removing added programs and files, identifying systems whose password files were compromised, and returning the systems to their original configurations so that no systems are left in a compromised condition. Further, general results from OA-20 penetration testing will be briefed only to key DOE managers outside of the field organization with a clear need to know (e.g., Secretary of Energy, Deputy Secretary of Energy, Director, Office of Security and Emergency Operations, and Lead Program Secretarial Officer). Note that OA-20 may share data with the Office of the Inspector General to meet the Government Information Security Reform Act audit requirements.

Terms of Testing

- OA-20 will provide the site with all information regarding the systems used for scanning and testing activities to prevent testing activities from being confused with real attacks and to minimize any risk associated with performance testing activity. OA-20 will maintain frequent communications with the site on the status of testing activities, and will expeditiously (to the greatest extent possible) report significant vulnerabilities as they are discovered and validated. OA-20 will coordinate with the designated site technical personnel to assist the site in taking immediate corrective actions. Additionally, OA-20 will employ a continuous self-assessment process to ensure strong security practices to preserve the integrity and confidentiality of collected assessment data.
- OA-20 will coordinate all activities with a designated site point of contact. While OA-20 will not attempt to exploit "denial of service" vulnerabilities (unless specifically requested by competent authority) and every attempt will be made to prevent damage to any information system and the data it holds, some penetration attempt scenarios have the possibility of causing service interruption or system damage. In the unlikely case that such an event occurs, OA-20 will work with the site to determine the nature of the problem and restore the system to its desired state of operation. OA-20 will not be held liable for damages in these cases.
- OA-20 will suspend all testing at the request of the site because of legitimate safety, security, or operational concerns. The site and OA-20 will work together expeditiously to resolve any concern so that remote vulnerability testing can resume as quickly as possible.

Appendix D

- OA-20 is authorized to access any available information related to system/network operation and security configuration (i.e., connectivity information, authentication data, and security parameters) on site networks being tested. During external testing, OA-20 will be authorized to access any site files, including user files, on computers or networks.
- After completing the external network assessment, the site will provide OA-20 with the necessary technical data to conduct a thorough tabletop review of firewall rules, border router access control lists, and intrusion detection capabilities. OA-20 will coordinate with the site to determine whether information regarding vulnerabilities would have been available other than by review of the rules.
- OA-20 will provide the DOE Computer Incident Advisory Capability with information regarding the systems used for scanning and testing activities to ensure that testing activities are not confused with real attacks.
- During the offsite testing, the site should maintain the normal operating posture of the external network security perimeter (e.g., border routers, firewalls, and intrusion detection systems). OA-20 will conduct vulnerability scans and attempt penetrations of the site's network over the Internet from its testing laboratory. Because OA-20 external performance testing is conducted overtly in a compressed timeframe, it is not designed to be a true test of intrusion detection capabilities. As such, the site will not manually reconfigure their network defenses to block testing activities by incorporating OA-20 Internet Protocol (IP) addresses in access control lists, firewall rule sets, and/or intrusion detection strings, or other perimeter cyber security technologies, as a means of explicitly blocking and/or filtering testing activities. If the site has automated processes in place to block hostile activities as part of its normal perimeter defense, these systems may remain in place; however, if OA-20 cannot obtain the vulnerability data necessary, the site and OA-20 will work together on a solution. If an OA-20 IP address is blocked during vulnerability scanning or penetration testing, an assessment team member will contact the site and have the block removed. The site will provide documentation of how OA-20 testing activities were identified.
- Intrusion detection capabilities will be assessed using a tabletop review. The site will provide information on intrusion detection architecture, strategies, and methodologies (including parameters, deployment locations, platforms, etc.) to facilitate this review.
- If OA-20 personnel are identified by any site personnel during testing activities, site cyber security personnel should inform them that the activity is associated with an authorized test. Site personnel should document the detection of activity and provide logs to OA-20 for tabletop analysis of intrusion detection capabilities. If there is any confusion or question as to the origin of scanning or penetration activities detected, normal site procedures for incident handling and reporting will be followed until resolution.
- The site will provide a listing of the range of phone numbers and all external and internally controlled IP addresses associated with site business, as well as topology maps blueprinting the cyber security infrastructure of the network. The site will validate all IP address ranges provided so as to help ensure that third-party entities will not be inadvertently scanned. When requested, OA-20 will exclude certain critical systems (e.g., safety systems, major applications undergoing upgrades or other special evolutions) from all testing activities. The site should provide specific network addresses and reasons for exclusion as an attachment to the signed performance test. Similarly, the site should provide a list of phone numbers and reason for exclusion from modem testing. The site will be responsible for providing phone and IP range information, along with proposed exclusions, to OA-20 prior to the beginning of the performance-testing window specified on the first page of this agreement. The site will be liable for any consequences associated with providing inaccurate information.
- The site will identify any systems or network nodes that are connected to the network(s), but are not under the direct control and responsibility of the site. Similarly, the site will identify any phone numbers that are not under the direct control and responsibility of the site. These systems will be excluded from testing unless OA-20 obtains permission from the system owner. The site will be

responsible for providing this information to OA-20 prior to the beginning of the performance-testing window specified on the first page of this agreement.

- It is the site's responsibility to restore network computer systems to a secure configuration after OA-20 testing. OA-20 will coordinate with and provide assistance (as requested) to system administrators during network computer systems "cleanup." Cleanup may consist of removing added programs and files, identifying systems whose password files were compromised, and restoring systems to a secure configuration so that no systems are left in a compromised condition. OA-20 will maintain an accurate record of all testing activities to assist in this process.
- OA-20 will not modify or delete any content of user files on DOE computers and networks. Additionally, OA-20 will not intentionally access files that deal with medical or financial data, data protected by the Privacy Act, or IPs declared "off limits."
- As evidenced by their signature on this performance test agreement, line management certifies that DOE's Banner and Warning Policy has been implemented and that network computer users have, as a result, granted constructive consent to this type of activity.

Approvals:

Director, Office of Cyber Security and Special Reviews

DOE Line Management Representative

Contractor Representative

This page intentionally left blank.

APPENDIX E

**SUMMARY SHEETS FOR INTERVIEWS CONDUCTED AND
KEY DOCUMENTS REVIEWED**

This page intentionally left blank.