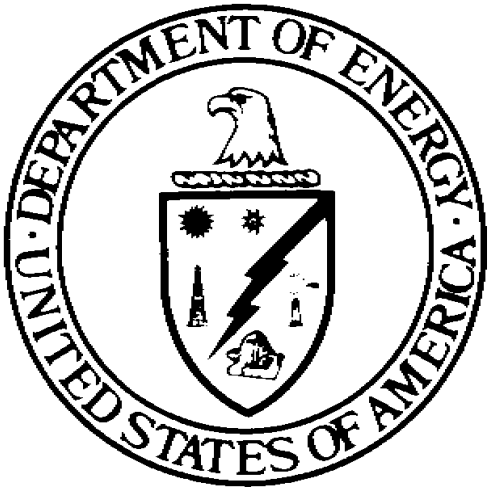
OFFICE OF INDEPENDENT OVERSIGHT
OFFICE OF CYBER SECURITY EVALUATIONS
APPRAISAL PROCESS GUIDE



April 2008
Office of Health, Safety and Security
U.S. Department of Energy

Preface

Department of Energy (DOE) Order 470.2B, *Independent Oversight and Performance Assurance Program*, and Office of Health, Safety and Security (HSS) Standard Operating Procedure, SOP-10-01, *Independent Oversight Appraisal Process Protocols*, February 2008, provide direction for the Office of Independent Oversight (HS-60) to establish the requirements, responsibilities, and processes for the development and maintenance of Appraisal Process Protocols that describe the activities for evaluating the effectiveness of DOE safeguards and security; cyber security; emergency management; and environment, safety, and health policies and of DOE line management in implementing those policies.

The HS-60 document, Independent Oversight Appraisal Process Protocols, describes the overall philosophy, approach, scope, and methods to be used by all HS-60 organizations when conducting Independent Oversight appraisals. Each subordinate office has developed and implemented specific procedures and techniques appropriate and necessary for accomplishing their unique responsibilities. This Office of Cyber Security Evaluations Appraisal Process Guide was developed for the purpose of documenting the appraisal approach and techniques specific to evaluations of classified and unclassified cyber security programs throughout DOE.

As part of the continuing effort to improve the Independent Oversight process, periodic updates and revisions will be made 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. Users of this document, as well as other interested parties, are invited to submit comments and recommendations to the Office of Cyber Security Evaluations.

Table of Contents

Acronyms

CAP	Corrective Action Plan
CIAC	Computer Incident Advisory Capability
DAA	Designated Approval Authority
DNS	Domain Name Server
DOE	U.S. Department of Energy
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSS	Office of Health, Safety and Security
HS-60	Office of Independent Oversight
HS-61	Office of Security Evaluations
HS-62	Office of Cyber Security Evaluations
IARC	Information Assurance Resource Center
IG	Office of the Inspector General
IP	Internet Protocol
ISSM	Integrated Safeguards and Security Management
NNSA	National Nuclear Security Administration
OCIO	Office of Chief Information Officer
PII	Personally Identifiable Information
PMA	Power Marketing Administration
POA&M	Plan of Action and Milestones
QRB	Quality Review Board
SSIMS	Safeguards and Security Information Management System
SSP	System Security Plan
TAP	Technical Assessment Protocol

Definitions

Cyber Security Appraisal: An umbrella term for an oversight activity to evaluate line management performance and the adequacy of policy related to cyber security and conducted by the Office of Cyber Security Evaluations; inspections, special reviews, and follow-up reviews are all forms of appraisals.

Corrective Action Plan (CAP): A document that provides, for each finding or deficiency addressed, a thorough analysis of the underlying causal factors to determine whether systemic program weaknesses exist, steps to address the cause(s) of the finding, detailed descriptions of the corrective action(s) to resolve each finding and prevent recurrence, and a general outline for the conduct of the proposed independent corrective action effectiveness review. For each corrective action, the document shows 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, deliverable(s) that will signify completion, and the mechanism(s) for verifying closure. A corrective action plan may also provide a detailed discussion of longer-term enhancements and upgrades, as well as descriptions of actions taken and compensatory measures already in place. For matters pertaining to Cyber Security, the CAP may also be referred to as a "Plan of Action and Milestones" (POA&M). [470.2B, FISMA]

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 of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Deficiency: A deficiency is an inadequacy that is found during an appraisal that does not meet the intent of a DOE policy, Federal or state law, or other applicable requirement (e.g., contract, standard, etc.). Deficiencies may serve as the basis for one or more findings. [470.2B]

Findings: Findings are used to indicate significant deficiencies or safety issues that warrant a high level of attention on the part of management. If left uncorrected, such findings could adversely affect the DOE mission, the environment, the safety or health of workers or the public, or national security. Findings may identify aspects of a program that do not meet the intent of DOE policy. Findings are clearly identified in the appraisal report, define the specific nature of the deficiency and whether it is localized or indicative of a systemic problem, and identify which organization is responsible for corrective actions. Findings require resolution by management through a formal corrective action process.

Integrated Safeguards and Security Management (ISSM): A formal, organized process for planning, performing, assessing, and improving the secure conduct of work in accordance with risk-based protection strategies as defined in DOE Policy 470.1, Integrated Safeguards and Security Management (ISSM) Policy. These systems are institutionalized through DOE directives and contracts. The ISSM system framework encompasses all levels of activities and documentation related to safeguards and security management throughout the DOE complex and includes all topical areas of safeguards and security (e.g., personnel, physical, information, and cyber security, and nuclear safeguards,) and related cross-cutting areas (e.g., export control, classification, foreign visits and assignments, and foreign travel). [470.1]

National Security Interests: Activities performed at DOE or DOE contractor, subcontractor, consultant, or other facilities or installations that involve classified matter, special nuclear materials, nuclear

weapons, nuclear weapons components and devices, critical infrastructure, or government property of high value or that would impact DOE program continuity, or otherwise are deemed important.

Performance Testing: The testing or exercising of an assessment object under specified conditions to compare actual with expected behavior, and using the results to support the determination of effectiveness of security controls. Technical performance testing is the evaluation, at the time of the test, 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 programmatic review represents the combined evaluation of data collected during the inspection, which includes examination of policy and documents, conduct of structured interviews with key personnel, review of data centers, sample of work stations, and the overall assessment of the management, operations, and technical controls that implement the cyber security program for a selected DOE site office or contractor site.

Validation : The process by which Independent Oversight ensures the factual accuracy of collected data and ensures that identified deficiencies, and their impacts, are effectively communicated to responsible managers and organizations.

Section 1 – Introduction

Cyber Security Evaluations Mission

The Office of Independent Oversight (HS-60) 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, HS-60 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 470.2B, Independent Oversight and Performance Assurance Program). For each of these areas, HS-60 follows a common set of overall appraisal protocols as described in the Office of Independent Oversight Appraisal Process Protocols.

This document, Office of Cyber Security Evaluations Appraisal Process Guide, provides additional insight into the Office of Cyber Security Evaluations (HS-62) 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.

HS-62 is responsible for implementing the Independent Oversight function of the DOE in matters related to cyber security. The activities of HS-62 encompass:

- Periodic inspections of classified and unclassified cyber security programs at DOE sites
- Periodic inspections of classified and unclassified cyber security intelligence programs at DOE sites
- A program of remote testing for DOE network vulnerabilities through scanning and penetration testing
- Unannounced penetration testing, commonly referred to as red teaming, of DOE sites
- 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
- Reviews 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 Federal Information Security Management Act (FISMA)

- Annual evaluations of classified information security programs for DOE as required by FISMA.

About This Guide

The Office of Cyber Security Evaluations Appraisal Process Guide is a subordinate document to the HS-60 Appraisal Process Protocols. While the HS-60 Appraisal Process Protocols provides general guidance common to the appraisal activities of all four of its offices, this document provides detail and guidance regarding procedures and methods specific to cyber security appraisals conducted by HS-62. DOE Order 470.2B is the reference document that defines program requirements, appropriate site response to identified vulnerabilities, and the corrective action plan development process. Since these documents should be used together, every effort has been made to avoid unnecessary duplication. HS-62 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. HS-62 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, HS-62 will develop a project plan to guide the appraisal or special study.

Scope of Cyber Security Evaluation Activities

To accomplish assigned responsibilities, HS-62 inspectors conduct various types of appraisals that may include program reviews, technical assessments, special reviews, and external network security assessments. The type and frequency of scheduled reviews are based on overall HS-60 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 can include 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.

Technical Assessments

External Penetration Testing

- Announced Testing Activities – Announced penetration testing is typically conducted in conjunction with a scheduled cyber security assessment of a facility. Announced activities are primarily used to provide an overall assessment of a site's network security posture. These assessment activities are conducted remotely from HS-62's Cyber Security Testing Network facilities. HS-62 external penetration testing consists of:
    - Scanning network systems exposed to the Internet for vulnerabilities and attempting exploits to evaluate the potential impact of weaknesses
    - Scanning site telephones using a war-dialer to identify unauthorized or misconfigured modems that could provide an alternative route into the network
    - Scanning site wireless networks to identify unauthorized or misconfigured wireless access that could provide an alternative route into the network.
- Unannounced Penetration Testing (red teaming) – Red teaming is primarily used to evaluate a site's ability to withstand focused attacks from Internet sources. The key aspect to red teaming is that the site is not informed of the inspection beforehand. However, HS-62 does work with "trusted agents" at the site to coordinate activities and to assure that any areas of the site network that should be excluded from testing activities are known to the HS-62 team in advance.

Internal Penetration Testing

- The key goal of internal penetration testing is to evaluate the strength of internal boundaries that provide isolation between differing need-to-know environments. Internal penetration testing is typically conducted during the onsite phase of an announced inspection. Testing may be conducted using site-provided systems, HS-62 mobile assets, or a combination of both. HS-62 technical personnel are provided a location from which most scanning and penetration testing activities are conducted. However, some testing may need to be conducted from various points within the site's network. Internal penetration testing may also be conducted in conjunction with a red team evolution, in which case it will be carefully coordinated with the trusted agent.

Special Reviews

Special studies and reviews conducted by HS-62 focus on cross-cutting cyber security functions and program 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 may include multiple sites allowing HS-62 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.

Section 2 – Cyber Security Appraisals

Introduction

The HS-62 appraisal program provides a standard, practical approach to assessing cyber security throughout the DOE complex, with the goal of evaluating the management, operational, and technical controls that are implemented to protect information technology resources and the information contained therein. Processes are continually reviewed, refined over time, and applied according to the level of protection needed. Processes, procedures, and tools used are also adjusted, modified, and updated to keep current with new tools and with the threats that new cyber technology introduces. This allows HS-62 to use government and industry best practices to ensure that cyber security is appropriately applied and that adequate protection measures are established for a secure operating environment.

As described in the Appraisal Process Protocols, all HS-60 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.

Approach to Cyber Security Appraisal Activities

HS-62 has established a systematic approach for cyber security appraisal activities that includes examination of the management, operations, and technical controls and performance testing in order to conduct thorough and objective assessments. Team members use a variety of assessment methods and performance tests 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. 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, the Office of Cyber Security Evaluations 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 approach results in the identification of systemic issues and provides a basis for evaluating the direction and sustainability of cyber security programs.

The HS-62 technical team personnel conduct extensive internal and external performance testing to evaluate the effectiveness of protection measures for classified and unclassified networks. HS-62 utilizes a technical standard operating procedure and technical assessment protocol (TAP) to ensure a consistent technical approach to cyber security performance testing. The technical standard operating procedure is an internal HS-62 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 the HS-62 approach to performance testing activities is provided in Appendix A, and a sample TAP is provided as Appendix D.

HS-62 programmatic reviews are focused on both program direction and program implementation of the management, operational, and technical components for analysis of overall effectiveness. Program direction is evaluated by assessing how well both DOE and contractor line management satisfy key responsibilities, and whether the resources, policies, and expectations for performance are adequate. Program implementation is evaluated using an evaluation framework and lines of inquiry to help structure interviews, data collection, analysis, and other inspection activities. Appendix B contains this evaluation framework which is utilized for cyber security program reviews.

HS-62 cyber security inspection results are routinely presented around the framework and categories of management, operations, and technical aspects described in Appendix B to assure a thorough assessment and report that identifies both positive aspects of program direction and implementation, as well as barriers to effective performance.

Appraisal Goals and Philosophy

The HS-60 oversight goals and philosophy stated in HS-60 Appraisal Process Protocol, Section 2, are adopted by HS-62 to guide appraisal activities.

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, HS-62 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 resources, are issued to line management if an appraisal identifies significant weaknesses that contribute to inadequacies in cyber security protection.

HS-62 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 HS-62 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.

Appraisal Standards

HS-62 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, HS-62 evaluates compliance with these requirements in the context of a performance-based review that uses extensive functional testing.

While the evaluation framework used by HS-62 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. The list of policies that HS-62 may reference is contained in Appendix C. As part of HS-62's responsibility to evaluate the effectiveness of DOE cyber security policy, a finding may be issued against a Headquarters organization or program office for the lack of effective policy.

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. The effectiveness of local standards is evaluated during the course of onsite programmatic reviews.

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 HS-62 organizational and assessment assignments.

Director, Office of Cyber Security Evaluations

The Director of HS-62 has responsibility for the following key functions and tasks:

- Implement HS-62 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 inspections when designated by the Director, Office of Independent Oversight
- Make cyber security appraisal team assignments and establish review scope
- Participate on the Quality Review Board (QRB)
- Brief senior DOE management and other stakeholders on appraisal results.

Deputy Director, Office of Cyber Security Evaluations

The Deputy Director of HS-62 has responsibility for the following key functions and tasks:

- Provide direction and guidance consistent with the HS-62 Director
- Recommend appraisal schedules
- Serve as Inspection Team Chief for inspections when designated by the Director, Office of Independent Oversight

- Support HS-62 Director in interfacing with Headquarters and field personnel to coordinate activities and address concerns
- Recommend appraisal team structure and scope
- Participate on the QRB
- Brief senior DOE management and other stakeholders on appraisal results.

Team Leader/Topic Team Leader

The HS-62 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 the recommended appraisal scope
- Provide direction and guidance to team members on the approach to specific appraisal activities
- Draft the 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
- 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 HS-62 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 the 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 HS-62 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 the direction and guidance of the Team Leader/Topic Team Leader or Technical Lead
- Assist in preparing 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.

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 must be cordial, open, and professional to provide maximum value. It is in the interest of both HS-62 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.

Section 3 – Appraisal Process Planning

Introduction

For different types of appraisal activities, the pre-planning 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 or a joint inspection with the Office of Security Evaluations (HS-61) or other HS offices.

When scheduling an inspection, an initial step involves identifying and assigning resources for the activity. The HS-62 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 HS-62 Director to ensure the thoroughness and rigor of the inspection.

During HS-61 safeguards and security inspections that involve a joint appraisal with HS-61, the HS-62 Team Leader/Topic Team Leader will also operationally report to the Inspection Team Chief. The Director of the Office of Independent Oversight designates an Inspection Team Chief for the inspection, who serves as the senior DOE official managing the evaluation activities and the senior HS-62 point of contact with the site being inspected. The Inspection Team Chief might be from HS-61, HS-62, or another HS office for combined appraisal activities. In any case, the Inspection Team Chief, HS-62 Director, and HS-62 Team Leader/Topic Team Leader are responsible for closely integrating activities into a single inspection activity. During joint inspection activities, HS-62 will follow general appraisal procedures established by HS-61 and documented in the Security Appraisal Process Guide.

The HS-62 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 HS-62 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 Team Leader/Topic Team Leader and Technical Leader work with the HS-62 Director to develop document requests, inspection and interview schedules, and the TAP document that the HS-62 Director and DOE Operations/Site Office representative sign. TAP is discussed in more detail below. Team members are assigned to support the programmatic and technical parts of the review as needed.

For integrated appraisals, the Inspection Team Chief will be the primary point of contact for the HS team and will make the necessary arrangements with the site for space, logistics, and other common team needs. For an HS-62-only appraisal, the Team Leader/Topic Team Leader will have 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 HS-62 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, operations, and technical program.

Pre-planning Phase

Pre-planning activities are initiated by the Director of HS-62, 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, Office of Cyber Security Evaluations and the Inspection Team Chief for joint HS-61and HS-62 appraisals to ensure that pre-planning activities are effectively conducted.

The HS-62 team conducts pre-planning by becoming familiar with the site organization, reviewing documentation, and developing an approach to the appraisal. There also may be a pre-planning meeting or telephone conference to assist in focusing the upcoming appraisal. Pre-planning 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 TAP
- 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 pre-planning 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. HS-62 routinely begins performance testing during the planning phase of the inspection after the TAP 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 request
- 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 Director, Office of Cyber Security Evaluations and the Inspection Team Chief (for joint HS-61and HS-62 inspections) on progress and specific approaches.

Technical Assessment Protocol

The TAP document outlines the respective roles and responsibilities of the Independent Oversight staff, Federal and contractor site's cyber security managers and trusted agents for the performance testing. The TAP explains the general approach and defines specific parameters and controls that will be followed during testing. Appendix D contains an example of the TAP. The performance test agreement must be signed by the HS-62 Director and a designated Federal representative prior to beginning any performance testing. All TAPs include the following general controls that HS-62 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, provide detailed information and work with the site 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) and National Nuclear Security Administration Information Resource Assurance Center (IARC) of performance testing start and stop dates to ensure that testing activities are not confused with real attacks.

As part of establishing a TAP, the site is responsible for informing HS-62 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, HS-62 may exclude some cyber systems from performance testing activities. HS-62 also conducts performance testing of telephone systems and conducts a search for wireless access points to look for access into the

site's network. Specific telephone numbers may be excluded from HS-62 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 HS-62 inspection team will request various documents and items of information. HS-62 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 the 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, firewall rules, and intrusion detection/prevention rules
- Information related to any wireless networks in use to include Service Set Identifier and Media Access Control addresses of all authorized access points
- Diagram of the classified computer network(s).

Programmatic Review Document Request. The HS-62 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:

- Current Program Cyber Security Plan and Cyber Security Program Plan being used for cyber security management, and other relevant site-specific management documents
- Security plans or master plans that describe the cyber security protection measures for computer systems, facsimiles, copiers, printers, and portable information technology devices
- Organization 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 (within the last 2 years) assessments, surveys, self-assessments, and reviews for classified and unclassified cyber security programs

- Any documentation on cyber security lessons-learned program
- Issue tracking reports, corrective action plans, plan of action and milestones reports
- Site-specific threat assessment information
- Risk assessment documents
- Documented risk mitigation strategies
- 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 relative to cyber security and information technology
- Site cyber security policies and procedures
- Documents that explain cyber security training program objectives for users and cyber security and information technology professionals.

Inspection Plan

For each inspection, HS-62 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 HS-62 conducts joint inspection activities with HS-61, a joint inspection plan will be developed by the Inspection Team Chief with input from the HS-62 Team Leader/Topic Team Leader and concurred upon by the HS-61and HS-62 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 HS-60, is sent to the site prior to the onsite appraisal.

Onsite Inspection Schedule

The inspection schedule is designed to efficiently use the limited time on site and ensure a thorough appraisal. The schedule must address 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 if indicated by events or the data collected or 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 HS-62 inspection team will schedule informal validation meetings with site 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 senior site management (e.g., security director, the Chief Information Officer) is held each day to briefly discuss the progress of the programmatic review and performance testing. For joint HS-61and HS-62 activities, the Inspection Team Chief is responsible for conducting the management meeting. The HS-62 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 pre-planning and planning efforts include:

- TAP
- 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 HS-62 inspection teams. The purpose of the augmentation program is to help improve the performance of cyber security management programs throughout DOE by:

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

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

- Detailed knowledge of Independent Oversight'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 the appraisal 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 augmentee program, HS-62 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 teams. Participants involved in the technical review typically have an extensive background in network performance testing. Similarly, participants involved in the programmatic portion of the HS-62 inspections must be knowledgeable of DOE orders, policies, and initiatives. HS-62 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. HS-60 will review each nominee's qualifications, interview each nominee, and make the final decision on each nominee's acceptance into the program.

A nominated augmentee's participation in an inspection will be arranged on a case-by-case basis, according to HS-62'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 significant business connections. Independent Oversight will pay travel expenses associated with augmentee participation in Independent Oversight appraisal activities. Home organizations/employers must pay each augmentee's salary.

Section 4 – Conducting Appraisals

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, HS-62 uses a "bottom-up" approach to program assessment. As a first step, cyber security appraisals typically begin with extensive external and internal 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 HS-62's Cyber Security Testing Networks. HS-62 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 noted in the Planning Section, HS-62 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, HS-62 conducts 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 HS-62 normally reaches assessment conclusions based on analysis of data, develops a draft report, and validates information with site personnel.

Goal

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

Performance Testing

The approach to performance testing activities is described in Appendix A. Performance testing is a key element of HS-62 cyber security appraisals since it provides tangible feedback on the current effectiveness of a site's cyber security protection posture. However, performance testing by itself does not allow for valid conclusions on the direction or sustainability of the program. Effectiveness and stability 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 combination of extensive performance testing and a review of essential program elements that allows HS-62 to fully and effectively assess unclassified and classified cyber security programs.

Any misuse of computer systems detected during performance testing is reported immediately to site management. If criminal activity is suspected, HS-62 reports this information to the Office of the Inspector General (IG) for investigation and resolution. HS-62 does not investigate alleged criminal activity or misconduct. The site is responsible for reporting computer security incidents to program officials, CIAC or IARC, and other organizations, as appropriate. Likewise, HS-62 is responsible for coordinating performance testing activities with CIAC or IARC.

Programmatic Review

Inspectors 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 implementation of management, operations, and technical controls.

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, HS-62 evaluates the effectiveness of DOE cyber security policy and provides feedback to DOE's Office of the Chief Information Officer and, as relevant, to the National Nuclear Security Administration Cyber Security Program Manager. In some cases, policy findings may be included in a site inspection report. HS-62 also evaluates DOE program office and site office performance as it relates to implementation of the cyber security program.

Communications and Feedback

HS-62's objective throughout each appraisal activity is to ensure that a thorough and accurate assessment of a site's cyber security program is conducted and that site personnel gain maximum benefit from the experience. To accomplish this, HS-62 personnel, site managers, and site cyber security staff must all communicate extensively. During both performance testing and programmatic reviews, HS-62 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 HS-62 personnel when concerns over factual accuracy exist. The site should provide additional data and identify site personnel who can help HS-62 personnel to identify corrections for any factual accuracy misunderstanding. The following activities are integrated into the HS-62 appraisal process to ensure that the inspection team and site managers and staff have an opportunity to effectively communicate:

- During remote performance testing, HS-62 technical personnel are in contact with site personnel routinely to discuss the status of testing and any issues.

- When conducting onsite programmatic and technical team review activities, the HS-62 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 HS-62 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 joint appraisals with HS-61, HS-62 provides an initial draft inspection report to the site for review and comment prior to departing the site. Otherwise, the draft report is transmitted to the site for review and a conference call is set up to discuss factual accuracy. HS-62 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, HS-62 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.

- HS-62 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 implementing cyber security measures or products to use. As part of its effort to help DOE sites, HS-62 is open to conducting a dialogue on technical issues. As an Independent Oversight organization, HS-62 does not direct a site to take any specific action, use any specific cyber security tools, or adopt any specific technical solutions. Rather, HS-62 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.

Section 5 – Appraisal Closure

Introduction

The closure phase of an inspection typically occurs after data collection (document reviews, interviews, and performance testing) is essentially complete. HS-62 inspectors follow the process described in the HS-60 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 develop logical, supportable conclusions that portray a fair picture of how well a cyber security program functions to protect classified and unclassified DOE information and 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 specific weaknesses identified during appraisal activities associated with the 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 requirements 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 an individual rating for each of the following areas: management, operations, and technical. Criteria for assigning ratings are stated in the HS-60 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 HS-62 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.

The Office of Independent Oversight uses a three-tier rating system that is intended to provide line management with a tool for determining where resources might be applied toward improving cyber security. It is not intended to provide a relative rating between specific facilities or programs at different sites because these reviews use a sampling technique to evaluate management systems and programs. The rating system helps to communicate performance information quickly and simply. The three ratings and the associated management responses are:

- Significant Weakness: Indicates senior management needs to immediately focus attention and resources necessary to resolve programmatic and/or technical weaknesses identified. A Significant Weakness rating within the management, operational, or technical category would normally reflect a number of significant findings that degrade a program's overall effectiveness and/or that are longstanding deficiencies that have not been adequately addressed. A Significant Weakness rating would, in most cases, warrant immediate action and compensatory measures as appropriate.

- Needs Improvement: Indicates a need for improvement and a significant increase in attention to programmatic and/or technical weaknesses. This rating is anticipatory and provides an opportunity for line management to correct and improve performance within the management, operational, or technical category before it results in a significant weakness.

- Effective Performance: Indicates effective overall performance in a cyber security program. There may be specific findings or deficiencies within the management, operational, or technical category that require attention and resolution, but that do not degrade the overall effectiveness of the system or program.

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 has been collected and information that has been validated during the "conduct phase" of the appraisal.

- An HS-60 QRB 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 HS-60 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 (four hours) to review the initial draft report and to 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. HS-62 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 QRB is established as an internal process that provides a fresh set of eyes for the review of draft reports from a management perspective prior to review by the Director of HS and then the site. The QRB 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 HS appraisal activities. The QRB is typically chaired by the Director of HS-60 and includes the HS-62 Director, and other senior personnel as directed. For joint appraisals with HS-61, the Director of HS-61 would also be included on the board.

Briefings

Part of the closure process includes briefing line management on the results and conclusions of the appraisal activity. Prior to leaving the site, HS-62 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 HS-62 Director (or Deputy) and Team Leader/Topic Team Leader will travel to the site (or arrange a conference call), after receiving factual accuracy feedback on the initial draft report, to brief management on the results.

Process Improvements

HS-62 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. The Team Leader/Topic Team Leader is responsible for soliciting feedback from each team member and making recommendations to the HS-62 Director on process improvements.

Independent Oversight also solicits feedback from DOE field and contractor line managers to ensure that the appraisal process provides value to site personnel. HS-62 welcomes any feedback on how appraisal processes can be improved to make them more effective.

Section 6 – Appraisal Follow-up

Introduction

The HS-60 Appraisal Process Protocol and DOE Order 470.2B 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. HS-62 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, HS-60 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 Intelligence and Counterintelligence. A strategy for conducting Headquarters briefings will be developed after each appraisal.

HS-62 may be requested to provide briefings to external stakeholders such as members of Congress, congressional committees, 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

HS-62 follows the requirements established by DOE Order 470.2B and guidance in the HS-61 Appraisal Process Guide on formal comments associated with the factual accuracy of final draft appraisal reports. HS-62 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. HS-62 personnel will communicate the disposition of comments to site personnel. After the resolution of final comments, HS-62 will publish the final report in accordance with HS-60 procedures.

Corrective Action Plans

Sites should follow the requirements established by DOE Order 470.2B, and guidance in the HS-60 Appraisal Process Protocols in developing corrective action plans in response to findings identified in HS-62 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 plan of action and milestones, updating the corrective action status, and closing findings. Independent Oversight 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, those findings will be tracked separately. HS-62 will monitor the progress of corrective actions through the conduct of follow-up reviews and subsequent appraisals.

Section 7 – Records Management

Documentation of Appraisal Activities

In conducting the inspection, HS-62 inspectors collect a large volume of data and information through performance testing, document reviews, and interviews. While HS-62's appraisal processes are designed to assure the factual accuracy of information presented in assessment reports, information is retained to provide supporting evidence. This documentation of results is necessary, considering that one aspect of HS-62'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 FISMA. This process includes an audit by the IG to validate HS-62 appraisals. Retention of key documentation is necessary to provide IG auditors with the information necessary to independently reach the same conclusions as contained in HS-62 appraisal reports. Each member of an HS-62 appraisal team has a role in documenting assessment activities for use in the development of conclusions.

The HS-62 Team Leader/Topic Team Leader is responsible for ensuring that key appraisal information is captured and retained. As a rule, HS-62 will not retain large volumes of information in support of documenting appraisal activities. If classified interview sheets or performance testing results are retained, all security requirements for the marking and handling of classified documents will be strictly followed. The HS-62 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 or not it should be retained. To prevent managing large quantities of paper documents, a high-speed scanner will be used 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 HS-62 Director in support of IG audits and other valid reasons. Specific information that must be retained from an inspection may vary, depending on the type of review, but will typically include:

- Inspection Plan
- Correspondence pertinent to the appraisal
- Approved TAP agreement
- Document request list and data call response
- Schedules of interviews conducted
- Network architecture diagrams and other relevant technical data
- Copy of technical data presented to the site
- Daily summaries
- Final drafts of reports.

To support the organization of information that is retained from an appraisal, the HS-62 Team Leader/Topic Team Leader will ensure that the required documentation is retained for the HS-62 file.

Appendix A – 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 pre-determined "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 to 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 employs 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's Office of Cyber Security Evaluations (HS-62) 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

HS-62 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). HS-62 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. HS-62 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 appropriate site personnel. Once this general network information is compiled and analyzed, HS-62 identifies individual system vulnerabilities.

A.3 Vulnerability Scanning

During this phase, HS-62 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, nessus, and/or manual techniques (e.g., telnet, FTP or file transfer protocol, or sendmail login banners). From this information, HS-62 develops a list of probable vulnerabilities associated with each potential target system. Also, at this point, HS-62 develops or compiles automated scripts to attempt exploitation of vulnerabilities.

HS-62 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.

HS-62 attempts to identify any wireless networking devices (client and server) that may be at a particular site. In the event that wireless networking is used, HS-62 will attempt to access the wireless network by exploiting configuration errors or weak encryption technologies.

A.4 Network Penetration Testing

Using information from network mapping and automated scanning, HS-62 attempts to access systems behind the Internet firewall(s) to evaluate the effectiveness of barriers intended to protect against external threats. HS-62 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 HS-62 penetration testing team. The strength of captured password files will be tested using password-cracking tools. If an account is compromised, HS-62 attempts to gain the privileges of a "super user," root, or administrator.

Since the goal of HS-62 testing is to determine the extent of vulnerabilities, and not simply to penetrate a single site system, HS-62 can use information discovered on one system to gain access to additional systems that may be "trusted" by the compromised system. Additionally, HS-62 may exploit host-level vulnerabilities to elevate privileges within the compromised system to install "sniffers" or other utilities. In either case, HS-62 may copy additional files during testing, if necessary, to determine the sensitivity of the information contained on the system.

A.5 Reporting

HS-62 maintains detailed records of all attempts to exploit vulnerabilities and activities conducted during performance testing. The results of HS-62 scans and penetration testing are provided to established points of contact so the site can take corrective actions to address identified vulnerabilities. HS-62'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.

HS-62'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 Evaluations and Inspection Protocol

Scope: The cyber security inspection evaluates the effectiveness, accountability, and overall performance of cyber security programs implemented by DOE and contractor line management and staffs in the protection of classified and unclassified information systems for confidentiality, integrity, and availability of information processed, stored, or transmitted.

Program Management and Implementation: The inspection lines of inquiry are largely aligned with Federal directives and guidance, relevant public law, Office of Management and Budget policies, National Institute of Standards and Technology guidance, and more specifically with DOE orders and directives. Inspection activities include reviews of documentation, interviews with managers and implementers, and performance testing of classified and unclassified networks, general support systems, and applications. The lines of inquiry are organized into the categories of management, operations, and technical criteria, and security controls that are graded by defined levels of consequence of loss for classified information and levels of concern for unclassified information and systems.

Performance Testing: For each inspection, a technical assessment protocol (TAP) is used to establish an agreement between the Office of Cyber Security Evaluations (HS-62) and designated management officials of the facility to be inspected. The TAP constitutes the formal agreement that establishes the rules of engagement for the Independent Oversight testing team and the facility's Federal and contractor management, and the information technology and cyber security staff. The TAP also contains the specific framework for testing and the certification, accreditation, and approval of tools and techniques that may be used for testing the subject systems and networks.

1.0 Management Controls

Management controls in the cyber security program are those controls that focus on risk reduction, planning, acquisition, and certification and accreditation of systems. Setting priorities, assuring efficient use of resources, and specific reports on the status of the program are key to the effectiveness of management controls at a facility.

1.1 Line Management Responsibilities and Authority

- Has the Program Office provided current policy and a Program Cyber Security Plan to Federal and contractor management at the site?
- Has the Program Office established expectations for performance, provided resources, and monitored the Federal oversight of the cyber security program at the site?
- Has the Program Office established expectations for performance, provided resources, and monitored the cyber security program at the site?
- Has the Site Office established clear priorities, expectations, and defined formal roles, responsibilities, authorities, and interfaces required for management of the cyber security program?
- Does the Site Office conduct cyber security surveys and technical assessments of performance?

- Have the appropriate DOE cyber security directives been incorporated into contracts or other binding agreements to ensure timely implementation by contractors and subcontractors?

- Has the contractor line management established the cyber security program with appropriate roles, responsibilities, clear implementing procedures, and performance initiatives?

- Have adequate cyber security resources (e.g., people, hardware, software) been allocated to the cyber security and information technology groups to support the efficient use of information technology that is consistent with cyber security requirements?

- Have appropriate cyber security program goals been established and are they being tracked to accomplishment through performance metrics?

- Are expectations for contractor and subcontractor cyber security performance linked to financial incentives and used effectively to achieve an effective cyber security program?

1.2 Risk Management

- Risk Assessment Policy and Procedures: Has the site issued a formal risk assessment policy and implementing procedures to facilitate implementation of the risk management process?

- Security Category: Has the site determined the levels of concern, in accordance with Federal Information Processing Standards (FIPS) 199 for unclassified systems, and determined the consequence of loss for information groups of national security systems? Have designated senior-level officials reviewed and approved the security categories? Has the site developed a threat statement?

- Risk Assessment: Has the site conducted a risk assessment to determine the magnitude of harm that could result from the loss of confidentiality, integrity, or availability of the information or systems that support the operations and assets of the facility?

- Residual Risk: Have residual risks been identified and used by the Designated Approval Authority (DAA) in the accreditation decision?

- Risk Assessment Update: Have the risk assessments been updated at least every three years or whenever there are significant changes to the information system, the facilities, or other conditions that may impact the security or accreditation status of the system?

- Vulnerability Scanning: Have regular scans for vulnerabilities for classified and unclassified information networks and systems been performed at least at the frequency documented in the system security plan (SSP) and when alerted to new vulnerabilities that could affect the system?

1.3. Planning

- Security Planning Policies and Procedures: Has the site issued a formal security planning policy and implementing procedures to facilitate the implementation of security planning and controls?

- Accreditation Boundaries and System Inventories: Have accreditation and system boundaries been appropriately defined and approved at the site management or DAA level? Are the boundaries correlated to the level of concern or consequence of loss?

- System Security Plan: Has the site developed and implemented security plans for the information systems that include an overview of the security requirements and describe the security controls in place or planned for meeting those requirements? Has the DAA approved the security plans?

- System Security Plan Update: Are the SSPs reviewed at least annually and revised to address system/organizational changes or problems identified during annual security assessments?

- Rules of Behavior: Has the site developed, implemented, and made available to all users, a set of rules that describes their responsibilities and expected behavior for use of information systems?

- Privacy Impact Assessment: Has a privacy impact assessment been conducted on applicable information systems that contain protected personally identifiable information?

- Security-Related Activity Planning: Does the site coordinate security-related activities (e.g., assessments, audits, system hardware and software maintenance, security certifications, testing/exercises) in order to minimize and reduce the impact on operations?

1.4. System Acquisition

- System and Services Acquisition Policy: Has the site issued a formal acquisition policy and procedures for the acquisition and control of information technology resources?

- Allocation of Resources: Has the site determined, documented, and allocated as part of its capital planning and investment control process the resources required to adequately protect information and information technology resources?

- System Inventory: Are system inventories maintained for program management purposes and for reporting purposes?

- Life Cycle Support: Does the system development life cycle process used in the management of information technology include information security considerations?

- Acquisitions: Are cyber security requirements and specifications included in information technology acquisition contracts for hardware, software, services, etc?

- Information System Documentation: Do specifications include administrator and user guides and sufficient vendor detail for analysis and testing of controls?

- Software Usage Restrictions: Has the site established policies and procedures in regard to appropriate software usage?

- User Installed Software: Does the organization enforce explicit rules governing the installation of software by users?

- External Information System Services: Does the site require third-party providers of information system services to employ adequate security controls?

1.5. Certification and Accreditation

- Certification and Accreditation Policies and Procedures: Has the site issued a formal certification and accreditation policy and procedures for implementation of required controls?

- Information System Connections: Has the site explicitly authorized all connections to an information system from outside of the accreditation boundary, and has it monitored/controlled the system connections on an ongoing basis?

- Security Certification: Has a certification test and evaluation of the security controls in the information system been conducted to determine the extent to which the controls are operating as intended and meeting security requirements? Has an independent certification agent or team conducted a test and evaluation for moderate and high-impact systems?

- Plan of Action and Milestones: Has the site developed and updated (quarterly) a plan of action and milestones (POA&Ms) for information systems that documents actions to correct identified deficiencies?

- Security Accreditation: Has the site authorized (i.e., accredited) each information system for processing before operations and updated the authorization (at least every three years) or upon significant change to the system?

1.6 Self-Assessments and Continuous Improvement

- Self-Assessments: Has the site conducted self-assessments at least annually to evaluate the status of the implementation of security controls and the overall effectiveness of the cyber security program?

- Continuous Monitoring: Has the site continuously monitored the effectiveness and adequacy of system controls via system scans, any external security assessments, configuration management, and management of POA&Ms and other DAA-directed means of monitoring systems?

1.7 Federal Information Security Management Act (FISMA) Reporting

- FISMA Reporting: Has the site tracked the progress of improvement initiatives through a POA&M and reported the number of systems (classified and unclassified) and the required security status of systems quarterly through the program office to the Chief Information Officer to meet the FISMA reporting requirements?

2.0 Operational Controls

Operational controls are those controls that are primarily implemented and executed by people (as opposed to systems). Operational controls include those associated with the security of personnel, physical environment, contingencies, configuration, maintenance, integrity, media, reporting of incidents, awareness, and training.

2.1 Personnel Security

- Personnel Security Policy and Procedures: Has the site issued a formal personnel security policy and procedures associated with cyber system users and maintainers?

- Position Categorization: Has the site assigned a risk designation to all categories of positions and established screening criteria for individuals filling those positions?

- Personnel Screening: Has the site required all personnel to be subject to an appropriate screening process prior to permitting access to information and information system resources?

- Personnel Termination: When employment is terminated, does the site terminate the user's system access, conduct exit interviews, and retrieve all system-related property in a timely manner?

- Personnel Transfer: Does the site review information systems/facilities access authorizations when personnel are reassigned or transferred to other positions and take appropriate actions?

- Access by Foreign Nationals: Does the site coordinate with the local Safeguards and Security Program to ensure that cyber access by foreign nationals is integrated with the specific requirements of DOE Order 142.1, *Classified Visits Involving Foreign Nationals*, and DOE Order 142.3, *Unclassified Foreign Visits and Assignments Program*?

- Access Agreements: Has the organization completed appropriate access agreements (e.g., non-disclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements) for all individuals with access to information systems?

- Third-Party Personnel Security: Does the site comply with personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system services, outsourced applications, and network and security management)?

- Personnel Sanctions: Has the site established and enforced a formal sanctions process for personnel failing to comply with local cyber security policies and procedures?

2.2 Physical and Environmental Protection

- Physical and Environmental Protection Policy and Procedures: Has the site issued a formal physical and environmental protection policy and procedures to facilitate controls associated with information systems?

- Physical Access Authorizations: Does the site maintain current lists of personnel with authorized access to facilities containing cyber systems and issued appropriate authorization credentials?

- Physical Access Control: Does the site control all physical access points (including entry/exit points) and verify access authorization to the facilities containing information systems?

- Access Control for Transmission Medium: Does the site control physical access to information system distribution and transmission lines within organizational facilities?

- Access Control for Display Medium: Does the site control physical access to information system devices that display information to prevent unauthorized individuals from observing the output?

- Visitor Control: Are visitors to the area containing information systems escorted and monitored?

- Access Records: Does the site maintain appropriate visitor access records to the facilities containing information systems?

- Power Equipment and Power Cabling: Does the site protect power equipment and power cabling for the information system from damage and destruction?

- Emergency Shutoff: Does the site provide the capability of shutting off power to any information system component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment?

- Emergency Power: Does the organization provide a short-term uninterruptible power supply to facilitate an orderly shutdown in the event of a primary power source loss?

- Fire Protection: Does the site employ and maintain fire suppression and detection devices/systems for data centers?

- Temperature and Humidity Controls: Does the site regularly maintain, within acceptable levels, and monitor the temperature and humidity within facilities containing information systems?

- Water Damage Protection: Does the site protect the information system from water damage resulting from broken plumbing lines by providing master shutoff valves?

- Delivery and Removal: Does the site control cyber-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintain appropriate records of those items?

- Information Leakage: For high-impact systems, does the organization protect the information system from information leakage due to electromagnetic signal emanations?

2.3 Contingency Planning

- Contingency Planning Policy and Procedures: Has the site issued a formal contingency planning policy and procedures to facilitate implementation of contingency planning controls?

- Contingency Plan: Has the organization developed and implemented a contingency plan for each information system that addresses contingency roles, responsibilities, assigned individuals with contact information, and activities for restoring the system?

- Contingency Training: Does the organization train personnel in their contingency roles and responsibilities and provide refresher training at least annually?

- Contingency Plan Testing: Does the organization test the contingency plan at least annually? Does management review the test results and initiate corrective actions?

- Contingency Plan Update: Is the contingency plan reviewed at least annually and revised if needed, based on the results of testing?

- Alternate Storage Site: Has the site identified an alternate storage site to permit the storage of information system backup information? Is it geographically separate from the primary storage site?

- Alternate Processing Site: Has an alternate processing site been identified to permit the resumption of impact information systems operations for critical mission/business functions as specified by the SSP and ITCP when the primary processing capabilities are unavailable?

- Telecommunications Services: Have the primary and alternate telecommunications services been identified to support information systems and have necessary agreements been initiated to permit the resumption of information systems operations for critical mission/business functions when the primary telecommunications capabilities are unavailable?

- Information System Backup: Does the site conduct backups of user-level and system-level information at least at the frequency specified in the Program Cyber Security Plan?

2.4 Configuration Management

- Configuration Management Policy and Procedures: Has the site issued a formal configuration management policy and procedures to facilitate implementation of the contingency planning policy and controls?

- Baseline Configuration: Has the site developed, documented, and maintained a current baseline configuration of the information system and an inventory of the system's constituent components? Does the site update the baseline configurations and inventory as part of information system component installations?

- Configuration Change Control: Are changes to information systems documented and controlled? Have appropriate organizational officials approved information system changes?

- Monitoring Configuration Changes: Are changes to information systems monitored and are security impact analyses conducted to determine the effects of the changes?

- Access Restrictions for Change: Are access restrictions enforced that are associated with changes to the information system? Are automated mechanisms used to enforce access restrictions?

- Configuration Settings: Are the security settings of information technology products configured to the most restrictive mode consistent with information system operational requirements?

- Least Functionality: Are information systems configured to provide only essential capabilities, and is the use of functions, ports, protocols, and/or services specifically prohibited and documented in the SSP?

- Information System Component Inventory: Does the organization develop, document, and maintain a current inventory of the components of the information system and relevant ownership?

2.5 System Maintenance

- System Maintenance Policy and Procedures: Has the site issued a formal information system maintenance policy and procedures to facilitate management of maintenance controls?

- Controlled Maintenance: Does the site schedule, perform, and document routine preventive and regular maintenance on the components of the information system?

- Maintenance Tools: Does the organization approve, control, and monitor the use of information system maintenance tools and maintain the tools on an ongoing basis?

- Remote Maintenance: Does the organization authorize, monitor, and control all remotely executed maintenance and diagnostic activities, if employed?

- Maintenance Personnel: Does the organization maintain a list of personnel authorized to perform maintenance on the information system? Are only authorized personnel allowed to perform maintenance on the information system?

- Timely Maintenance: Does the organization obtain maintenance support and spare parts for its key information systems components within the maximum allowable outage or timeframe to support mission requirements?

2.6 System and Information Integrity

- System and Information Integrity Policy and Procedures: Has the organization issued a formal system and information integrity policy and procedures to facilitate management of controls for system and information integrity?

- Flaw Remediation: Does the organization identify, report, and correct information system flaws, and is information on identified flaws reported to the DOE Cyber Incident Advisory Capability or the National Nuclear Security Administration Information Assurance Response Center?

- Malicious Code Protection: Has the site implemented malicious code protection that includes a capability for automatic updates?

    - Information System Monitoring Tools and Techniques: Does the site employ tools and techniques to monitor events on the information system, detect attacks, and provide identification and notification of unauthorized use of the system? Does the site require Internet access points to have network-based intrusion detection systems and require all Internet-accessible servers to have host-based intrusion detection systems in place and functioning?

    - Does the information system provide a real-time alert when indications of compromise or potential compromise occur?

- Security Alerts and Advisories: Does the organization receive information system security alerts/advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response?

- Software and Information Integrity: Does the information system detect and protect against unauthorized changes to software and information?

- Spam and Spyware Protection: Does the information system implement spam and spyware protection?

- Information Input Restrictions: Does the organization restrict the capability to write information to the information system to authorized personnel?

- Error Handling: Does the information system identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries?

- Information Output Handling and Retention: Does the organization handle and retain output from the information system in accordance with Departmental file retention or operational requirements?

2.7 Media Protection

- Media Protection Policy and Procedures: Has the site issued a formal media protection policy and procedures to facilitate management and control of media protection?

- Media Access: Do only authorized users have access to information in printed form or on digital media removed from the information system?

- Media Labeling: Are external labels affixed to removable storage media and system output indicating the distribution limitations, handling caveats, and applicable security markings?

- Media Storage: Are information system media (paper and electronic) physically controlled and securely stored in accordance with the highest security category of the information recorded on the media?

- Media Transport: Does the site control information system media (paper and electronic) and restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel?

- Media Sanitization and Disposal: Are approved equipment, techniques, and procedures followed to sanitize information system media, both digital and non-digital, prior to disposal or release for reuse?

2.8 Incident Response

- Incident Response: Has the site issued a formal incident response policy and procedures to facilitate implementation of the incident response controls?

- Incident Response Training: Does the site train personnel in their incident response roles and responsibilities for the information system and provide refresher training?

- Incident Response Testing and Exercises: Is the incident response capability tested at least annually to determine effectiveness?

- Incident Handling: Has an incident handling capability for security incidents been implemented that includes preparation, detection and analysis, containment, eradication, and recovery?

- Incident Monitoring: Are incidents tracked and documented on an ongoing basis?

- Incident Reporting: Is incident information promptly reported to appropriate authorities?

- Incident Response Assistance: Does the site provide an incident response support resource that offers advice and assistance to users for the handling and reporting of security incidents?

2.9 Security Awareness and Training

- Security Awareness and Training Policy and Procedures: Has the site issued formal security awareness and training policy and procedures to facilitate implementation?

- Security Awareness: Is basic security awareness training provided to all information system users (including managers and senior executives) before granting access to the system, and at least annually thereafter?

- Security Training: Does the site identify personnel who have significant security roles and provide security training before authorizing access to the system or performing assigned duties? Are training plans executed for these personnel?

- Security Training Records: Are individual training activities documented and monitored?

- Contacts with Security Groups and Associations: For high-impact systems does the organization maintain contacts with peer groups and professionals to stay up to date with the latest recommended security practices and information about threats, vulnerabilities, and incidents?

3.0 Technical Controls

Technical controls are primarily implemented and executed through mechanisms contained in the hardware, software, or firmware components of the system. Technical controls include identification, authentication, access control, audit, accountability, and system communications.

3.1 Identification and Authentication

- Identification and Authentication Policy and Procedures: Has the site issued formal identification and authentication policy and procedures to facilitate implementation?

- User Identification and Authentication: Do information systems uniquely identify and authenticate users (or processes acting on behalf of users)? Is multi-factor authentication required for privileged and remote system access?

- Device Authentication: Does the information system identify and authenticate specific devices before establishing a connection?

- Identifier Management: Are user identifiers managed to uniquely identify and verify each user, based on authorization from the user's manager? Is the user identifier disabled after a reasonable period of inactivity?

- Authenticator Management: Are authenticators managed with procedures for initial creation, distribution, event of loss, and revocation? Are default authenticators changed upon information system installation? Does the site enforce changing/refreshing authenticators periodically?

- Authenticator Feedback: Does the information system obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals?

- Cryptographic Module Authentication: Does the system employ authentication methods that meet the DOE requirements for authentication to a cryptographic module? (including FIPS 140-2, as amended)

3.2 Access Control

- Access Control Policy and Procedures: Has the site issued a formal access control policy and procedures to facilitate effective performance of access controls?

- Account Management: Are information system accounts managed to control the establishing, activating, modifying, reviewing, disabling, and removing accounts? Are accounts reviewed and revalidated at a reasonable frequency?

- Access Enforcement: Does the information system enforce assigned authorizations for controlling access to the system in accordance with applicable policy?

- Information Flow Enforcement: Does the information system enforce assigned authorization for controlling the flow of information within the system and between interconnected systems?

- Separation of Duties: Does the information system enforce separation of duties through assigned access authorizations?

- Least Privilege: Does the information system enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for their specific job?

- Unsuccessful Login Attempts: Does the information system enforce a limit on number of consecutive invalid access attempts by a user during a specified time period?

- System Use Notification: Does the information system display an approved system use notification message (warning banner) before granting system access?

- Session Lock: After a specified period of inactivity, does the information system initiate a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures?

- Session Termination: Does the system automatically terminate the session after a period of inactivity that is specified in the SSP?

- Permitted Actions Without Identification or Authentication: Are the specific user actions identified and documented that can be performed without identification or authentication?

- Automated Marking: For high-impact systems, is output automatically marked using standard naming conventions to identify any special dissemination, handling, or distribution instruction?

- Remote Access: Does the site authorize, monitor, and control all methods of remote access to information systems?

- Wireless Access Restrictions: Does the site establish usage restrictions and implementation guidance for wireless technologies, and authorize, monitor, and control wireless access to information systems?

- Access Control for Portable and Mobile Devices: Does the site establish usage restrictions and implementation guidance for organization-controlled portable and mobile devices?

- Use of External Information Systems: Does the site restrict the use of personally owned systems?

3.3 Audit and Accountability – Lines of Inquiry

- Audit and Accountability Policy and Procedures: Has the site issued a formal audit and accountability policy and procedures to facilitate implementation of controls?

- Auditable Events: Does the SSP define what events generate audit records for the system?

- Content of Audit Records: Does the information system produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events?

- Audit Storage Capacity: Is sufficient audit record storage capacity allocated and configured to reduce the likelihood of storage capacity being exceeded?

- Response to Audit Processing Failures: In the event of an audit processing failure, are appropriate organizational officials alerted to take appropriate actions as specified by the SSP for shutdown, overwrite, or other course of action?

- Audit Monitoring, Analysis, and Reporting: Are audit records regularly reviewed for indications of inappropriate or unusual activity, and are suspicious activities or suspected violations investigated and findings reported to appropriate officials for necessary action?

- Audit Reduction and Report Generation: Does the system provide an audit reduction and report generation capability?

- Time Stamps: Does the information system provide time stamps for use in audit record generation?

- Protection of Audit Information: Does the information system protect audit information and audit tools from unauthorized access, modification, and deletion?

- Audit Record Retention: Are audit logs retained for at least the time period specified in the SSP or at least one year?

3.4 System and Communication Protection – Lines of Inquiry

- System and Communications Protection Policy and Procedures: Has the site issued a formal system and communications protection policy and procedures to facilitate management and protection of communications?

- Application Partitioning: Does the system separate user functionality (including user interface services) from information system management functionality?

- Security Function Isolation: Does the system isolate security functions from non-security functions?

- Information Remanence: Does the system prevent unauthorized and unintended information transfer via shared system resources?

- Denial of Service Protection: Does the system protect against or limit the effects of denial of service attacks?

- Boundary Protection: Does the information system monitor and control communications at the accreditation boundary and at key internal boundaries within the system?

- Transmission Integrity: Does the system protect the integrity of transmitted information?

- Transmission Confidentiality: Does the system protect the confidentiality of transmitted information?

- Network Disconnect: Does the system terminate a network connection at the end of a session or after a period of time specified in the SSP?

- Trusted Path: For classified systems, is a trusted communications path implemented to provide a secure communication path between users and the system security controls, to protect data from modification or disclosure, and for use in the initial user authentication to the system and resources?

- Cryptographic Key Establishment and Management: When cryptography is required for use in the system, are cryptographic keys established and managed using manual procedures or automated mechanisms with supporting procedures?

- Use of Cryptography: When cryptography is used within the information system, are all cryptographic operations (including key generation) performed in accordance with FIPS 140-2 for unclassified, and DOE Manual 205.1-3 for classified systems?

- Public Access Systems: Does the system protect the integrity and availability of publicly available information and applications?

- Collaborative Computing: Does the information system prohibit remote activation of collaborative computing mechanisms and provide an explicit indication of use to the local users?

- Transmission of Security Parameters: Does the information system reliably associate security parameters with information exchanged between information systems?

- Public Key Infrastructure Certificates: Does the site issue public key certificates under an approved certificate policy or obtain public key certificates under an appropriate certificate policy from an approved service provider?

- Mobile Code: Are usage restrictions established for mobile code technologies, and does the site authorize, monitor, and control the use of mobile code within the information network?

- Voice over Internet Protocol: Are usage restrictions and implementation guidance established for Voice over Internet Protocol (VoIP) technologies, and does the site authorize, monitor, and control the use of VoIP within the information network?

- Secure Name and Address Resolution Service (authoritative source): Does the system that manages the name/address resolution service provide additional data origin and integrity artifacts along with the authoritative data it returns (i.e., digital signatures and cryptographic keys)?

- Secure Name and Address Resolution Service (recursive or caching resolver): Does the system that provides name/address resolution service for local clients perform data origin authentication and data integrity verification on the responses it receives from authoritative sources?

- Architecture and Provisioning for Name/Address Resolution Service: Are the information systems that collectively provide name/address resolution service fault tolerant and do they implement role separation?

- Session Authenticity: Does the system provide mechanisms to protect the authenticity of communications sessions (e.g., in service-oriented architectures providing web-based services)?

Appendix C – Reference Documents

1. 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.

2. 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.

3. Public Law 104-106, Information Technology Management Reform Act Federal Information System Management Act (FISMA)

4. OMB Circular A-130, as amended, Management of Federal Information Resources, dated November 2003, as amended, promulgates policy and responsibilities for the development, implementation, and management of Federal information resources.

5. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), dated February 2006.

6. DOE Order 200.1, Information Management Program, dated 9-30-96, assigns responsibilities and authorities and prescribes policies, procedures, standards, and guidelines for the management of information, information resources, and information technology as a corporate asset integrated with programmatic planning and budgeting.

7. DOE Manual 200.1-1, Telecommunications Security Manual, dated 2-15-2000, provides general guidance for the use, review, coordination, and provision of telecommunications services for the DOE.

8. DOE Policy 205.1, Departmental Cyber Security Management Policy, dated 5-8-01, explains the DOE ISSM policy within the cyber security realm.

9. DOE Order 205.1A, Departmental of Energy Cyber Security Management, dated 12-4-06, establishes line management accountability through Senior DOE Management for ensuring protection of information and information systems, and prescribes that Senior DOE Management will manage and implement their respective cyber security programs through a Program Cyber Security Plan.

10. DOE Manual 205.1-4, National Security Systems Manual, dated 3-8-07, establishes security controls for the protection, control, and management of DOE classified information.

11. 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.

12. DOE Order 470.2B, Independent Oversight and Performance Assurance Program

13. DOE Order 471.1A, Identification and Protection of Unclassified Controlled Nuclear Information (UCNI)

14. DOE Order 471.3, Identifying and Protecting Official Use Only (OUO) Information

15. DOE Order 471.2A, Information Security Program, dated 3-27-97, establishes an Information Security Program for the protection and control of classified and sensitive information.

16. DOE Manual 475.1-1, Identifying Classified Information, dated 5-8-98, provides guidance for the management of the DOE classification and declassification program.

17. Senior DOE Management Program Cyber Security Plans for the DOE HQ, National Nuclear Security Administration (NNSA), Office of Science (SC), Office of Energy (E), and the Power Management Administration (PMA).

18. DOE CIO Cyber Security Technical and Management Requirements, TMR-0, DOE Cyber Security Program Foundation

19. DOE CIO TMR-1, Management, Operational, and Technical Controls

20. DOE CIO TMR-2, Certification and Accreditation

21. DOE CIO TMR-3, Risk Management

22. DOE CIO TMR-4, Vulnerability Management

23. DOE CIO TMR-5, Interconnected Systems Management

24. DOE CIO TMR-6, Plan of Action and Milestones

25. DOE CIO TMR-7, Contingency Planning

26. DOE CIO TMR-8, Configuration Management

27. DOE CIO TMR-9, Incident Management

28. DOE CIO TMR-10, Media Clearing, Purging, and Destruction

29. DOE CIO TMR-11, Authenticator Management

30. DOE CIO TMR-12, Wireless Devices and Information Systems

31. DOE CIO TMR-13, Portable and Mobile Devices

32. DOE CIO TMR-14, External Information Systems

33. DOE CIO TMR-18, Peer-to-Peer (P2P) Networking

34. DOE CIO TMR-19, Remote Access

35. DOE CIO TMR-21, Security Testing and Evaluation

36. DOE CIO TMR-22, Protection of Sensitive Unclassified Information, Including Personally Identifiable Information

37. NIST Federal Information Processing Standard (FIPS) Publication 140.2, Security Requirements for Cryptographic Modules

38. NIST FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems

39. NIST FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems

40. NIST Special Publication (SP) 800-18, Rev 1, Guide for Developing Security Plans for Information Technology Systems

41. NIST SP 800-30, Risk Management Guide for Information Technology Systems

42. NIST SP 800-34, Contingency Planning Guide for Information Technology Systems

43. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information

44. NIST SP 800-53, Rev 1, Recommended Security Controls for Federal Information Systems

45. NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004

46. An Overview of Department of Energy Cyber Security Threats, version .92, dated February 2007.

47. HS-62 SOP 102, Inspection Records Management Procedures, August 2006

Appendix D – Sample Independent Oversight Cyber Security Technical Assessment Protocol

OFFICE OF INDEPENDENT OVERSIGHT
CYBER SECURITY TECHNICAL ASSESSMENT PROTOCOLS
FOR UNCLASSIFIED NETWORK TESTING

SITE: SITE NAME

DATES: START – END DATE

OBJECTIVE:

The Office of Cyber Security Evaluations has been tasked to assess the security posture of the SITE NAME unclassified computer networks. Independent Oversight will conduct an in-depth technical assessment that includes security testing and review of network configuration parameters (e.g., firewall rules, border router access lists, intrusion detection architecture and system configuration, and security architecture). Security testing will include systematic probing of network defenses (both internal and external) to identify potential vulnerabilities as well as attempt to exploit any weaknesses discovered.

Specifically, Independent Oversight will:

1. Identify potential internal and external network, dial-up, and wireless vulnerabilities using various scanning techniques, manual processes, and thorough review of technical information.

2. Attempt exploitation of some, or all, identified vulnerabilities to evaluate whether they are true weaknesses.

ASSESSMENT PROCESS:

1.0 Identification of Vulnerabilities

1.1 External Unclassified Network Assessment

The purpose of the external network assessment is to determine the site's vulnerability to attack from an outside source. As part of the assessment, Independent Oversight will conduct network mapping and vulnerability scanning of the site's unclassified networks from Independent Oversight's Cyber Security Testing Network via the Internet. Remote testing will also include additional scanning to identify computer and network systems that contain vulnerabilities, or configuration anomalies, that could allow unauthorized access from the Internet. All information obtained by Independent Oversight will be protected from unauthorized access in accordance with DOE orders and applicable Federal requirements.

The site will continue to operate as normal, without taking any special actions to block Independent Oversight testing activities. Intrusion logs of any Independent Oversight events or activities should be kept by the site. Independent Oversight will assess the effectiveness of the site's intrusion detection system (IDS) and intrusion prevention system (IPS) during a tabletop review, to be held at a later time. For details, see "Technical Assessment Terms and Requirements," below.

Independent Oversight will use an automated modem search tool (war-dialer) to scan through the range of site telephone numbers. War-dialing will be accomplished from the Independent Oversight test network or by site-owned war-dialing equipment. At the discretion of Independent Oversight, recent site war-dialing records may be used to meet the requirement. The war-dialing tool will identify which, if any, of the telephone numbers are used for computer modems in "auto-answer" mode. Modems identified through war-dialing will be compared with the site's list of known modems and may be subject to penetration testing. War-dialing will be conducted during non-business hours (e.g., 5:00 PM – 6:00 AM) Monday through Friday and anytime on weekends, as necessary.

Independent Oversight will also conduct war-driving/walking to detect unauthorized wireless networks and to assess the security of authorized wireless networks. War-driving will utilize specialized antennas and laptops equipped with software for this purpose. Upon identification of a wireless network/device, Independent Oversight will follow approved internal procedures to determine (with a high degree of certainty) that the site owns the detected device. Once this determination has been made, Independent Oversight will attempt to connect to the wireless network and assess the security of the network and all connected systems. Wireless access points identified through war-driving will be compared with the site's list of approved wireless access points and may be subject to penetration testing.

As part of remote testing, Independent Oversight may also utilize a social engineering technique, referred to as a data-driven attack, to evaluate user awareness and to determine the ability of such an attack to subvert site perimeter defenses. This technique involves covertly delivering computer code (Trojan horse program) by e-mail or other means resulting in users causing the execution of that code through their overt actions. All plans for social engineering during the external network assessment phase of the assessment will be coordinated with the Trusted Agent before execution.

Independent Oversight scanning of the SITE NAME external network will begin on START DATE and continue until completed, not later than END DATE. If at any time a SITE NAME system becomes unavailable as a potential result of Independent Oversight scanning, Independent Oversight will immediately cease all scanning activity and contact the SITE NAME Trusted Agent. Scanning will resume when the Trusted Agent and Independent Oversight agree that it is safe to do so.

1.2 Internal Network Assessment

The purpose of the internal network assessment is to determine the network's vulnerability to attack from inside the network itself. For this part of the assessment, Independent Oversight will conduct vulnerability scanning and security testing of the site's network on site, using systems that are connected to the network. For details, see "Technical Assessment Terms and Requirements," below.

2.0 Exploitation of Identified Vulnerabilities

2.1 External Unclassified Network Assessment

Independent Oversight will evaluate the effectiveness of barriers (e.g., firewalls, proxies, host-level security features) that protect against external threats. Testing will be conducted on all potential pathways into the network, including Internet, modem, and wireless access points. Examples of vulnerabilities that may be exploited during security testing include, but are not limited to: buffer overflows, application or system configuration problems, routing issues, DNS attacks, cracking of captured passwords, address spoofing, share access, and exploitation of inherent system trust relationships. If Independent Oversight can compromise a user account, Independent Oversight will test that account for access permissions and will attempt to subvert systems into granting super user, root, or administrator access. Independent

Oversight may use any additional information discovered in order to gain access to other systems or targets. Independent Oversight may also install other attack tools or information-gathering tools to further the exploitation of other targets, depending on need and applicable protocols. Independent Oversight will fully document all applications installed by the inspection team on any systems, and report this information to SITE NAME contacts.

Independent Oversight may use compromised systems to gain access to other systems or networks. Independent Oversight will take precautions to minimize the potential for testing to result in damage, degradation, or debilitation of service on business systems. Independent Oversight testing will not result in the introduction of vulnerabilities to site systems. In those cases where Independent Oversight identifies vulnerabilities that already exist, Independent Oversight will expeditiously (to the greatest extent possible) report vulnerabilities that place sensitive information or systems at risk as they are discovered and validated so that systems will not be left vulnerable for extended periods of time. When the vulnerability appears not to place sensitive information or systems at direct risk, Independent Oversight will test the extent of the vulnerability before reporting the vulnerability to the site.

2.2 Internal Network Assessment

Scanning of unclassified networks to identify potential vulnerabilities will be conducted by Independent Oversight personnel using systems approved by the Designated Approving Authority (DAA). Independent Oversight will coordinate assessment strategies with designated Trusted Agents. As a rule, denial-of-service techniques will not be utilized during scanning or penetration testing. In some cases, however, Independent Oversight may need to force a system to restart to execute a particular exploit. This will only be done after careful coordination with the site Trusted Agent.

Independent Oversight will also assess the ability of an insider user to traverse unclassified networks and gain access to resources outside the boundaries of officially allocated privileges. In addition to internal vulnerability scanning, Independent Oversight will attempt to exploit system vulnerabilities. Examples of vulnerabilities that may be exploited during internal testing are similar to those previously described. These include, but are not limited to, cracking of captured passwords, shared access and exploitation of inherent system trust relationships, configuration problems, deploying "sniffers" to capture passwords, ARP spoofing, ARP poisoning, keystroke loggers, Trojans, and various computer forensic techniques that may reveal user and system login/account information. Independent Oversight will take precautions to minimize the potential for testing to result in damage, degradation, or debilitation of service.

REPORTING OF RESULTS:

Independent Oversight will provide the results of scans and security testing to designated site personnel to facilitate actions to correct identified vulnerabilities. Independent Oversight will also provide enough 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 systems are not left in a compromised condition. Further, general results from Independent Oversight security testing will only be briefed to key individuals with a need to know. It should be noted that Independent Oversight will share data with the Office of the Inspector General, if required, to meet the Federal Information Security Management Act (FISMA) audit requirements.

TECHNICAL ASSESSMENT TERMS AND REQUIREMENTS:

Information Requirements

- Independent Oversight requires a listing of the range of phone numbers and all externally and internally controlled IP addresses associated with site business, as well as topology maps blueprinting the cyber security infrastructure of the network(s). The site will validate all IP address ranges provided so as to help ensure that third-party entities will not be inadvertently scanned. The site may request that certain critical systems (e.g., safety systems, major applications undergoing upgrades or other special evolutions) be excluded from testing activities. Local DOE/site representatives are responsible for providing phone and IP information, along with proposed exclusions and justification, to Independent Oversight for consideration before the assessment begins. The site is liable for any consequences associated with providing inaccurate information.

- Independent Oversight requires a listing of any systems, network nodes, or phone numbers that are part of the site's address space, but are not under their direct control and responsibility. These systems will be excluded from testing unless Independent Oversight obtains permission from the system owner. Local DOE/site representatives are responsible for providing this information to Independent Oversight before the assessment begins and, if requested by Independent Oversight, obtaining permission from the system owner to allow Independent Oversight testing.

- Intrusion detection and prevention capabilities, firewall rules, and border router access control lists (ACLs) will be assessed using a tabletop review. Independent Oversight will require information on intrusion detection architecture, strategies, and methodologies; firewall rules and configuration files; and border router ACLs (including parameters, deployment locations, platforms, etc.) to facilitate this review. Independent Oversight will coordinate with site personnel regarding the time and manner in which this information will be made available. Independent Oversight will engage in technical discussions with appropriate site personnel to determine whether information regarding any vulnerability associated with this information would have been available other than by direct review.

- SITE NAME will provide device configuration data and vulnerability scan results as requested in the data call to Independent Oversight personnel at the time of the assessment.

Technical Assessment Protocols

- Independent Oversight encourages a site Trusted Agent to participate with the technical team in the security testing of the internal network to promote communication and understanding of the technical assessment.

- Independent Oversight will provide the site with 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 the security testing activity. Independent Oversight will maintain frequent communication with the Trusted Agent on the status of testing activities, and will expeditiously (to the greatest extent possible) report significant vulnerabilities that place sensitive information at risk as they are discovered and validated. Independent Oversight will coordinate with the Trusted Agent to assist the site in taking immediate corrective actions. Additionally, Independent Oversight employs a continuous self-assessment process to ensure strong security practices and to preserve the integrity and confidentiality of collected assessment data.

- Independent Oversight will coordinate all activities with the Trusted Agent. Every attempt will be made to prevent damage to any information system and the data it holds. Some assessment activities have the possibility of causing service interruption or system damage. SITE NAME can request the exclusion of important business and operational systems from testing if there are concerns regarding potential system interruption. If the Independent Oversight testing team or SITE NAME points of contact have concerns that testing may adversely effect network operations or result in damage to network components, discussions will be held prior to testing so that all parties agree on the appropriate course of action. In the unlikely case that system testing causes unanticipated consequences, Independent Oversight will work with site personnel to determine the nature of the problem and to restore the system to its desired state of operation. Independent Oversight will not be held liable for damages in these cases.

- If requested by DOE management at the site, Independent Oversight will temporarily suspend testing over legitimate safety, security, or operational concerns. The site and Independent Oversight will work together expeditiously to resolve any concern so that testing can resume as quickly as possible.

- Independent Oversight is authorized to access any available information related to system/network operation and security configuration (e.g., connectivity information, authentication data, and security parameters) on site networks being tested. During security testing, Independent Oversight is authorized to access any available site files, including user files, on computers or networks. Independent Oversight will not retain or disclose any Personally Identifiable Information (PII) encountered during the assessment. All information obtained by Independent Oversight during the course of the inspection will be protected consistent with Departmental directives for handling sensitive information.

- Independent Oversight, in coordination with a designated site point of contact, will conduct wireless network testing. The intent of this security testing activity will be to detect unauthorized wireless networks, and to assess the security of authorized wireless networks. Wireless security testing will include war-driving the perimeter of site building(s) utilizing directional antennas and laptops with specialized software for this purpose. Independent Oversight will attempt to bypass any encryption and/or authentication mechanisms in place on the wireless network to determine the internal network's susceptibility to attack through this vector. Additionally, Independent Oversight will attempt to determine if any sensitive information is being stored, processed, or transmitted on the wireless network.

- Independent Oversight will provide the DOE Computer Incident Advisory Capability (CIAC) and National Nuclear Security Administration Information Assurance Response Center (IARC) with information regarding the systems used for remote scanning and testing activities to ensure that testing activities are not confused with real attacks.

- During Independent Oversight remote testing, the site should maintain the normal operating posture of the external network security perimeter (e.g., border routers, firewalls, and intrusion detection/prevention systems). Independent Oversight will conduct vulnerability scans and attempt to access the site's network over the Internet from its Cyber Security Testing Network. The site will continue to follow standard operating procedures and will not reconfigure network defenses to block or filter testing activities through actions such as adding Independent Oversight IP addresses to ACLs, firewall rule sets, intrusion detection strings, and/or other perimeter cyber security technologies. If the site has normal operating procedures or automated processes in place to block hostile activities as part of its normal perimeter defense, these will remain in place.

However, if Independent Oversight cannot obtain the vulnerability data necessary, the site representatives and Independent Oversight will work together on a solution. If SITE NAME blocking mechanisms are activated, Independent Oversight will contact the Trusted Agent to unblock the addresses and stop any manual blocking procedures for Independent Oversight IP addresses. Site personnel will provide documentation of how Independent Oversight testing activities were identified and blocked.

- In the event that any site personnel identify Independent Oversight testing activities, site cyber security personnel should inform those personnel that the activity is associated with an authorized test. Site personnel should document the detection of activity and provide logs to Independent Oversight for tabletop analysis of intrusion detection capabilities. If there is any confusion or question as to the origin of scanning or testing activities detected, normal site procedures for incident handling and reporting should be followed until resolution.

- It is the site's responsibility to restore network and computer systems to a secure configuration after Independent Oversight testing. Independent Oversight will coordinate with and provide assistance (as requested) to system administrators during this period of "cleaning up" network computer systems. 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 systems are not left in a compromised condition. Independent Oversight will maintain an accurate record of all testing activities to assist in this process.

Local DOE Representative's Responsibilities

- The local DOE authorized representative must verify that the Department's Banner and Warning Policy has been implemented at the site being assessed and that network computer users have, as a result, granted constructive consent to the types of activities Independent Oversight performs in carrying out its assessment responsibilities.

- The local DOE authorized representative is responsible for coordinating Independent Oversight's cyber security technical assessment with the site being assessed and ensuring that the technical assessment protocols are followed. The local DOE authorized representative is also responsible for ensuring that all resource and information requirements to support this technical assessment are satisfied.

ACKNOWLEDGEMENT OF TECHNICAL ASSESSMENT PROTOCOLS FOR UNCLASSIFIED NETWORK TESTING:

_____

Designated Approving Authority for SITE NAME

_____

Director, Office of Cyber Security Evaluations,
Office of Independent Oversight

OFFICE OF INDEPENDENT OVERSIGHT
CYBER SECURITY TECHNICAL ASSESSMENT PROTOCOLS
FOR CLASSIFIED NETWORK TESTING

SITE: SITE NAME

DATES: START – END DATE

OBJECTIVE:

The Office of Independent Oversight will be performing a vulnerability assessment and penetration test of the SITE NAME classified network(s) in order to identify potential vulnerabilities, test some exploitation scenarios, and assess the impact of any vulnerabilities on the network's security posture.

Vulnerability Assessment

The vulnerability assessment will identify potential vulnerabilities through scanning of the SITE NAME classified network(s) as well as evaluating network architecture, firewall rules, router access control lists (ACLs), intrusion detection system signatures, operating system configurations, and auditing and logging mechanisms.

Penetration Testing

If vulnerabilities are identified, Independent Oversight will assess the likelihood that an authorized user of SITE NAME classified systems could exploit these vulnerabilities and violate need-to-know protection measures. Testing of some of those vulnerabilities will serve to assess the effectiveness of need-to-know barriers such as firewall rules; router ACLs; intrusion detection system signatures; operating system, user, group, file, and directory permissions; and file attributes.

The remainder of this document describes these two activities and how Independent Oversight will use the resulting information.

ASSESSMENT PROCESS:

1. Vulnerability Assessment

Scanning of the SITE NAME classified networks to identify potential vulnerabilities will be conducted by Independent Oversight personnel, under the direct supervision of designated SITE NAME personnel, using systems accredited by the Designated Approving Authority (DAA). All tools introduced into the classified networks' environment to facilitate testing will be approved by the DAA. As a rule, denial-of-service techniques will not be utilized during scanning or penetration testing. In some cases, however, Independent Oversight may need to force a system to restart to execute a particular exploit. This will only be done after careful coordination with the site Trusted Agent.

Independent Oversight scanning of the SITE NAME classified network(s) can begin as early as START DATE, and continue until completed, not later than END DATE. Independent Oversight will notify the DAA when testing has been completed.

2. Penetration Testing

For each specific penetration test scenario, specific details regarding the steps to be taken, the expected results, and any effects the evaluation will or may trigger will be discussed in detail prior to any actual testing. Penetration testing scenarios will be documented, including the introduction of any additional tools or scripts.

To minimize the risk of unintentional disclosure of information, all Independent Oversight testing activities on classified networks will be closely observed by designated SITE NAME Trusted Agent(s). Trained SITE NAME personnel familiar with the portion of the network being tested will be notified by the DAA and/or designated SITE NAME Trusted Agent(s) and will be on call to provide assistance as required.

Penetration testing conducted on the classified networks will adhere to the following guidelines:

- Performed by appropriate cleared Independent Oversight team members under the direct observation of designated SITE NAME Trusted Agent(s). The Trusted Agents assigned to observe testing activities should have extensive knowledge and experience with the specific operating systems and network management devices utilized on the network.

- Conducted using tools approved for use on the classified network.

- Conducted using systems accredited for use on the classified network.

- Approved by the DAA.

ASSESSMENT TERMS AND REQUIREMENTS:

Independent Oversight Responsibilities

- Independent Oversight will request and must receive DAA authorization for all testing tools to be installed on a classified system as part of the security test.

- Independent Oversight will not attempt to defeat need-to-know protection measures via surveillance equipment, social engineering, or TEMPEST attacks.

- Independent Oversight will maintain frequent communication with SITE NAME counterparts on proposed testing activities and tools needed to support testing.

- Independent Oversight will report significant vulnerabilities that place classified information at risk of compromise by uncleared personnel as they are discovered and validated. In such cases, Independent Oversight will notify the SITE NAME Trusted Agent, the cyber security manager, and the DAA. Independent Oversight will coordinate with designated SITE NAME technical personnel to assist the site in taking immediate corrective actions.

- Independent Oversight will coordinate all activities with the designated SITE NAME points of contact. Every attempt will be made to prevent damage to any information system and the data it holds. Some assessment activities may have the possibility of causing service interruption or system damage. In the unlikely case that such an event occurs, Independent Oversight will work

with site personnel to determine the nature of the problem and restore the system to its desired state of operation.

- Independent Oversight will temporarily suspend testing over legitimate safety, security, or operational concerns if requested by SITE NAME. SITE NAME and Independent Oversight personnel will work together expeditiously to resolve any concern so that testing can resume as quickly as possible.

SITE NAME Responsibilities

- SITE NAME will provide a listing of the range of internally controlled IP addresses associated with site classified network(s) as well as topology maps blueprinting the cyber security infrastructure of the network(s). The site may request that certain critical systems (e.g., safety systems, major applications undergoing upgrades or other special evolutions) be excluded from testing activities. Local DOE/site representatives are responsible for providing IP information, along with proposed exclusions and justification, to Independent Oversight for consideration before the assessment begins.

- SITE NAME will ensure that existing scan results are classified at the appropriate classification level prior to providing them to Independent Oversight. The scan results will be removed from the classified networks and made available to Independent Oversight by SITE NAME personnel in both an electronic and hard copy form in order to allow for detailed analysis.

- SITE NAME will not manually reconfigure network defenses to block testing activities by incorporating testing addresses in ACLs, firewall rule sets, intrusion detection strings, and/or other technologies, as a means of explicitly blocking and/or filtering testing activities.

- SITE NAME will provide information to the appropriate classified network system administrators and cyber security personnel (e.g., Information System Security Officers) regarding the system(s) used for scanning and testing activities to prevent testing activities from being confused with real attacks and to minimize any risk associated with the security testing activity.

- In the event that any network user or system administrator identifies ongoing testing activities, SITE NAME cyber security personnel should inform them that the activity is associated with an authorized test. Site personnel should document the detection of testing activities. 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 should be followed until resolution.

- It is SITE NAME's responsibility to restore network and computer systems to a secure configuration after testing. Independent Oversight will coordinate with and provide assistance (as requested) to system administrators during this period of "cleaning up" network computer systems.

Designated Approving Authority Responsibilities

- The DAA must verify that the Department's Banner and Warning Policy has been implemented on the network(s) being tested and that network computer users have, as a result, granted constructive consent to the types of activities Independent Oversight performs in carrying out its assessment responsibilities.

- Identification of any systems or network nodes that are connected to the classified networks, but are not under direct control and responsibility of the SITE NAME DAA. These systems will be excluded from testing unless Independent Oversight obtains permission from the applicable DAA.

- The DAA is responsible for approving use of the Independent Oversight Classified Attack DVD image and obtaining a suitably accredited system for its use.

- The DAA is responsible for coordinating Independent Oversight's cyber security technical assessment with the responsible site contractor and ensuring that the technical assessment protocols are followed. The DAA is also responsible for ensuring that all resource and information requirements to support this technical assessment are satisfied.

ACKNOWLEDGEMENT OF TECHNICAL ASSESSMENT PROTOCOLS FOR CLASSIFIED NETWORK TESTING:

_____

Designated Approving Authority for SITE NAME

_____

Director, Office of Cyber Security Evaluations,
Office of Independent Oversight

OFFICE OF CYBER SECURITY EVALUATIONS
CYBER SECURITY ONSITE TECHNICAL ASSESSMENT
RESOURCE REQUIREMENTS

For the onsite assessment, the Independent Oversight technical team will require support from site personnel. It is requested that the following items be set up and operational at the start of business on the first day of Independent Oversight's arrival on site:

Unclassified Requirements

- The Independent Oversight technical team will need a separate, lockable room with access to the site's internal unclassified networks. This space will be utilized for internal network security testing as well as an area for the technical team to conduct discussions and analyses. The location should be within close proximity to the Independent Oversight programmatic team, if at all possible. In addition to the necessary equipment and network connections, the room should contain:
    - A white board or chalkboard
    - Table and chairs
    - Telephone
    - Network switch
    - Two power strips
- Independent Oversight will need two site computer systems on the internal network to support the technical assessment. In addition, Independent Oversight will use its own laptop and portable systems, for which the site will provide full access to the unclassified network and to the Internet. The site-provided systems need to meet the following specifications:
    - One system running the latest version of Windows configured exactly as the site standard build for typical users.
    - One system running the latest version of Linux/Unix configured exactly as the site standard build for typical users.
- Access to the site network and the Internet for site and Independent Oversight-provided systems.
- Connections to network segments (e.g., user segment, server segment). These connections should have throughputs of at least 100Mbs. Independent Oversight will need 20 static IP addresses for the duration of the inspection.

Classified Requirements

- Independent Oversight will need two accredited scan systems pre-configured with the Independent Oversight Classified Attack DVD image, once it has been authorized by the DAA.
    - One system will be used for scanning the network(s).
    - One system will be used for validating scan results, viewing file directory contents, and manually evaluating need-to-know boundaries.

OFFICE OF CYBER SECURITY EVALUATIONS
MEMORANDUM OF UNDERSTANDING AND AGREEMENT
REGARDING TRUSTED AGENT RESPONSIBILITIES

This memorandum summarizes the purpose, duties, responsibilities, and relationships associated with the use of Trusted Agents in connection with the Office of Independent Oversight cyber security testing.

When conducting security tests in conjunction with announced cyber security reviews, the Office of Cyber Security Evaluations (Independent Oversight) typically employs one or more Trusted Agents – appointed by the inspected facility/organization/operations office – who observe the security tests. Independent Oversight welcomes the participation of these personnel and views this as an opportunity for site personnel to see the techniques and tools used by Independent Oversight and to view the interaction between the Independent Oversight team members. The Trusted Agents also provide a resource to the Independent Oversight team to provide immediate access to the site for any potential issues that may arise during the assessment. The Trusted Agent will also be able to provide significant insight into site processes that may mitigate some network vulnerabilities. Since the Trusted Agent represents his/her facility/organization and is privy to sensitive security testing information (e.g., vulnerabilities being exploited), it is important that the Trusted Agent understand the confidentiality requirements of the position.

Trusted Agents by their mere presence in the room with the Independent Oversight team will be privy to all details regarding security testing and as a result will know if particular systems are being targeted. The Trusted Agent must agree to maintain the details of the testing in strict confidence until the conclusion of the testing phase to allow for as complete a technical assessment as possible. The Independent Oversight team may take several days to conduct the tests that will consist of progressive steps of penetrating systems and to use any compromised system as a stepping-stone to evaluate further vulnerabilities. If the Trusted Agent reveals the direction and plan of any testing activities to site personnel, site personnel may in turn correct the vulnerabilities or take the vulnerable system off-line to prevent a full evaluation of a weakness. This action will hinder the ability of the Independent Oversight personnel to fully evaluate the cyber security posture of the site and will negate a full and accurate report to the site. At the conclusion of the testing, all data concerning systems exploited during testing activities will be provided to the site, and Independent Oversight will work with site personnel to identify and correct the vulnerabilities that were discovered.

To ensure an accurate and thorough assessment, it is imperative that the Trusted Agent and the Trusted Agent's management understand the need to protect the validity of the assessment through strict confidentiality of the operations, methods, and activities of the security testing. Site personnel, who are not Trusted Agents, should maintain their normal operations and should document Independent Oversight activities as they are discovered through their normal processes. Communication between the site personnel and the Independent Oversight testing team should be open and frequent as the security testing activities progress.

OFFICE OF CYBER SECURITY EVALUATIONS
MEMORANDUM OF UNDERSTANDING AND AGREEMENT
REGARDING TRUSTED AGENT RESPONSIBILITIES

Since these responsibilities place the Trusted Agent in a position that requires a high level of trust to be placed in him/her by both his/her own management and by Independent Oversight, it is important that all parties involved understand the Trusted Agent's position and agree to bestow or accept the necessary trust. The signatures below formally acknowledge this understanding and agreement.

Trusted Agent:

_____	_____	_____
Name	Position	Signature/Date

Trusted Agent's Manager:

_____	_____	_____
Name	Position	Signature/Date

SITE NAME Point of Contact:

_____	_____	_____
Name	Position	Signature/Date

Independent Oversight Representative:

_____	_____	_____
Name	Position	Signature/Date