U.S. DEPARTMENT OF
ENERGY

EA Enterprise Assessments

Office of Cyber Assessments

Assessment Process Guide

April 2025

Office of Cyber Assessments

Office of Enterprise Assessments

U.S. Department of Energy

Document Version Control			
Version Number	**Change Editor**	**Date of Change**	**Description of Changes Made**
1.0	EA-62 Advisory Group	March 26, 2020	Original Document
1.1	EA-62	September 10, 2020	Updates to clarify assessment types (onsite vs. remote) and editorial changes
1.2	EA-62	February 2, 2022	Updates consistent Assessment scoping SOP v2.0. Added EA-60 Deputy Director Roles and Responsibilities, updated EA-61 Director Roles, and Responsibilities. Other minor editorial changes.
1.3	EA-62	January 2023	Terminology updates to increase clarity related to report distribution. Remove role of "Federal assessment co-lead."
1.4	EA-60	June 2024	Annual review: Changes made to realign with process updates made throughout CY23 and remove Ops Manager
1.5	EA-60	April 2025	Updating CNS section to be the SCAN program.

Office of Cyber Assessments
Assessment Process Guide

Approval Form

Approved by:

CHRISTOPHER MCFEARIN

Digitally signed by CHRISTOPHER MCFEARIN
Date: 2025.04.29 05:44:53 -06'00'

Christopher E. McFearin
Director
Office of Cyber Assessments
Office of Enterprise Assessments

KIMBERLY KELLY

Digitally signed by KIMBERLY KELLY
Date: 2025.04.28 16:47:40 -04'00'

Kimberly A. Kelly
Deputy Director
Office of Cyber Assessments
Office of Enterprise Assessments

Acknowledged by:

[VACANT]
Director
Office of Cyber Assessment Strategy
Office of Enterprise Assessments

Timothy B. Schwab

Digitally signed by Timothy B. Schwab
Date: 2025.04.28 07:52:49 -04'00'

Timothy B. Schwab
Director
Office of Cyber Assessment Operations
Office of Enterprise Assessments

Table of Contents

Acronyms v
1 Introduction 1
2 Organization 2
2.1 Roles and Responsibilities 2
3 Collaboration with External Organizations 8
3.1 Augmentee and Observer Program 8
4 Assessment Types 9
4.1 Assessment Activities 10
4.1.1 Programmatic Assessment Activities 10
4.1.2 Technical Assessment Activities 10
4.1.3 Special Assessments 13
4.1.4 Other Assessment Activities 13
5 Assessment Phases 13
5.1 Initiating 13
5.1.1 Initiating Inputs and Outputs 14
5.2 Planning 15
5.2.1 Planning Phase Activities 15
5.2.2 Assessment Plan 17
5.2.3 Rules of Engagement 17
5.2.4 Programmatic Data Call 18
5.2.5 Technical Data Call 19
5.2.6 Logistics Information 20
5.2.7 Assessment Schedule 20
5.2.8 Planning Inputs and Outputs 21
5.3 Conducting 23
5.3.1 Technical Approach 24
5.3.2 Programmatic Approach 26
5.3.3 Communication and Feedback 26
5.3.4 Testing Conclusion Activities 27
5.3.5 Conducting Outputs 28
5.4 Reporting 29

5.4.1 Analysis of Results 29
5.4.2 Report Preparation 30
5.4.3 Collaborative Review Meetings 30
5.4.4 Draft Report Distribution for Factual Accuracy Review 31
5.4.5 Pre-QRB Collaborative Review 31
5.4.6 Quality Review Board 31
5.4.7 Finalizing the Report 31
5.4.8 Reporting Outputs 32
5.5 Closing 33
5.5.1 Process Improvement 34
5.5.2 Documentation of Assessment Activities 34
5.5.3 Records Retention 34
5.5.4 Closing Outputs 34
Appendix A: Definitions 36

Acronyms

ATO	Authorization to Operate
CISO	Chief Information Security Officer
CNSSI	Committee on National Security Systems Instruction
CSTN	Cyber Security Testing Network
DHS	Department of Homeland Security
DOE	U.S. Department of Energy
EA	Office of Enterprise Assessments
EA-1	Director, Office of Enterprise Assessments
EA-60	Office of Cyber Assessments
EA-61	Office of Cyber Assessment Strategy
EA-62	Office of Cyber Assessment Operations
FAR	Factual Accuracy Review
FedRAMP	Federal Risk and Authorization Management Program
FIE	Field Intelligence Element
FISMA	Federal Information Security Modernization Act
GC	Office of the General Counsel
HVA	High Value Asset
IARC	Information Assurance Response Center
IC	Intelligence Community
IG	Office of the Inspector General
iJC3	Integrated Joint Cybersecurity Coordination Center
IMGB	Information Management Governance Board
IN	Office of Intelligence and Counterintelligence
IP	Internet Protocol
ISSO	Information System Security Officer
IT	Information Technology
KD	Knowledge Development
KM	Knowledge Management
NIST	National Institute of Standards and Technology

NNSA	National Nuclear Security Administration
OCIO	Office of the Chief Information Officer
OFI	Opportunity for Improvement
POA&M	Plan of Action and Milestones
QRB	Quality Review Board
ROE	Rules of Engagement
SCAN	Systematic Correlation and Analysis of Networks Program
SSC	Support Services Contractor

1 Introduction

This document is a companion to the *Office of Cyber Assessments Program Plan.* The program plan outlines the authorities, implementation, and overall vision and mission for the Office of Cyber Assessments.

This Assessment Process Guide describes EA-60's techniques and procedures for evaluating DOE cybersecurity programs, including the NNSA and contractor organizations' protection of special nuclear material, classified information, Power Marketing Administrations, and sensitive unclassified information.

This Assessment Process Guide is part of an ongoing effort to maintain the quality, consistency, and contribution of the assessment program's activities and products. EA-60 has evolved the assessment process through experience and has developed this process guide to be flexible and easily adaptable as the EA-60 assessment teams apply it to assessment activities. To ensure that this guide remains current, and the assessment process continues to improve, EA-60 encourages all users of this guide to provide comments and recommendations to the EA-61 and EA-62 Directors for consideration.

This process guide applies to EA-60 team members responsible for conducting cybersecurity assessments and serves as a primary resource to ensure consistency in completing an assessment. This process guide will be reviewed and, if applicable, updated at least annually.

This document provides additional insight into the assessment approach and processes associated with assessing classified and unclassified cybersecurity programs. In general, EA-60's assessment activities encompass the following:

- Periodic assessments of classified and unclassified cybersecurity programs across DOE.
- Periodic assessments of DOE classified and unclassified cybersecurity intelligence programs.
- Remote testing of DOE internet-facing assets for weaknesses and/or vulnerabilities through scanning and technical performance testing.
- Unannounced technical performance testing of DOE systems and programs
- Open-source information gathering of DOE entities.
- Open-source threat information gathering and analysis.
- Maintaining ongoing situational awareness of DOE mission and project priorities and aligning assessment activities to those during planning.
- Follow-up activities to ensure that identified issues are addressed in a timely and effective manner.
- Ongoing analysis of assessments results to identify cybersecurity trends and emerging issues within DOE.
- Development of valuable recommendations and identification of opportunities for improving cybersecurity performance that consider threat information and mission impact.
- Reviews of other governmental and commercial cybersecurity programs and frameworks to provide benchmarks for DOE performance.
- Review of the effectiveness of DOE policies governing classified and unclassified cybersecurity.

- Providing inputs for the annual evaluation of DOE's national security systems and field intelligence elements (FIEs), as required by the Federal Information Security Modernization Act (FISMA) of 2014.
- Participation in various Departmental working groups to maintain situational awareness and provide subject matter expertise, they include but are not limited to:
    - Cyber and Information and Operational Technology Executive Council
    - DOE Information Management Governance Board (IMGB)
    - DOE Insider Threat Working Group
    - DOE Enterprise Architecture Governance Board
    - DOE Incident Response Leaders Forum
    - Chief Information Security Officer (CISO) Roundtable.

Applicable laws, orders, policies, and standards related to the overall assessment process can be found in the *Office of Cyber Assessments Program Plan*.

2 Organization

EA-60 is led by the Director and Deputy Director who oversees and monitors the operations of the office as well as maintaining situational awareness of key priorities of the department as well as capturing assessment feedback needed to improve the overall value to its stakeholders. EA-60 has two offices that work together to conduct cybersecurity assessments. The Office of Cyber Assessment Strategy (EA-61) and Office of Cyber Assessment Operations (EA-62) are led by their respective directors and work alongside one another to plan, conduct, and effectively report on the results from each unique assessment.

2.1 Roles and Responsibilities

Each member of the assessment team serves as an integral part of the assessment lifecycle. Table 1 lists the entities responsible for conducting assessment activities. Each person fulfilling one or multiple roles within the assessment process will acknowledge these responsibilities annually.

Table 1: Roles and Responsibilities

Role	Responsibility
EA-60 Director	• Approve assessment reports prior to distribution to the Director, Office of Enterprise Assessments (EA-1). • Distribute EA-1 approved reports to site management. • Provide insights into and feedback on the overall assessment process. • Serve as the Quality Review Board (QRB) chair for all EA-60 reports. • Serve as technical monitor for the support services contract. • Act as system owner for all assessment-related information technology (IT) resources.

Role	Responsibility
EA-60 Deputy Director	• Act on behalf of the Director when unavailable. • Monitor the implementation of the priorities for the assessment program and provide feedback to the Director. • Collaborate with other EA offices to share assessment results and trends. • Collaborate with other EA offices to identify areas for assessment collaboration. • Participate in DOE working groups and councils as a subject matter expert and to identify potential areas for additional assessment focus.
EA-61 Director	• Work with the EA-62 Director to define and integrate assessment planning, conduct, and reporting that align with DOE mission priorities. • Oversee and maintain the EA-60 Knowledge Management (KM) and Knowledge Development (KD) efforts to provide relevant information to inform the assessment process. • Provide threat information pertinent to each assessment for use as part of the initial planning and scoping process, development of assessment strategies, and reporting. • Provide trending information pertaining to cybersecurity assessments results. • In conjunction with EA-62, receive, process, and arbitrate new Federal requirements, DOE directives, policy, and other official guidance to make recommendations for inclusion into the assessment process. • Work with EA-62 to develop and maintain a process guide for conducting cybersecurity assessments (this document).

Role	Responsibility
EA-62 Director	• In collaboration with the EA-61 Director, provide overall direction and management for cybersecurity assessment operations within EA-60. • Brief DOE managers and senior officials – including the Under Secretaries, Secretarial Officers, EA-1, and the EA-60 Director – and DOE policy organizations on the results of assessment activities. • Notify the EA-60 Director when assessment activities identify concerns that may have criminal or waste/fraud/abuse implications. • Work with EA-61 to develop and maintain a process guide for conducting cybersecurity assessments (this document). • Ensure that subsequent cybersecurity assessment activities review the effectiveness of corrective actions using a tailored approach based on significance and complexity. • Work with cognizant DOE line managers and policy organizations to resolve disagreements on assessment schedules, results, findings, deficiencies, or opportunities for improvement (OFIs). • Participate in QRB meetings. • Provide coordination, coaching, and oversight of Federal assessment team leaders in the conduct of assessments. • Provide assessment results and other required information to the EA-61 to assist in trending and analysis. • Work with the EA-61 Director to integrate assessment strategies that align with DOE mission priorities. • Support the EA-60 KM and KD efforts to capture relevant information about the assessment process and provide the data to EA-61.

Role	Responsibility
Federal Assessment Team Leaders	• Lead assessments of cybersecurity programs or topics when assigned by either the EA-61 or EA-62 Director. • Provide direction and guidance to team members on the scope and approach to specific assessment activities. • Support the EA-61 and EA-62 Directors in interfacing with DOE Headquarters and field personnel to coordinate activities and address concerns. • Chair the collaborative review meetings for assessments they have led. • Lead adjudication of factual accuracy review (FAR) and QRB comments. • Lead discussion of comment adjudication in QRB meetings. • Lead assessment planning meetings and provide input to assessment activities. • Draft assessment-specific slides, cybersecurity assessment plans, data calls, and other assessment planning documents. • Manage site personnel's access to the online repository for data calls. • Coordinate logistics for the assessment, including requests for appropriate resources needed for the assessment. • Provide feedback on proposed assessment team structure and make recommendations for the allocation of resources needed to accomplish the scope, ensuring the assessment team is appropriately resourced to complete the assessment. • Coordinate with site POC (POC) for receipt of relevant documentation and artifacts prior to assessments. • Establish the schedule of events during cybersecurity assessments and deliver it to the site POCs. • Ensure that team members perform their assigned duties before, during, and after the assessment. • Address any concerns associated with assessment activities. • Provide feedback to site personnel daily to validate assessment information and clearly communicate areas of concern. • Provide feedback on the overall assessment during the post assessment meetings on what went well, what could be improved, and what we can change for next time. • Provide direction, including context, outcome, and impact during the development of the assessment report. • Review and provide direction and comments on the assessment report to ensure the report meets quality standards for value and accuracy and is appropriate for the intended audience. • Brief site management and cybersecurity personnel on assessment results. • Immediately notify EA-62 and EA-60 Directors of any impact related to assessment activities. • Brief EA and DOE senior management on assessment results. • Ensure the delivery of the report for FAR and QRB by the approved targets.

Programmatic and Technical Team Leaders	• Provide support in preparing the annual National Security Systems and Office of Intelligence and Counterintelligence (IN) FISMA reports. • Support the Federal assessment team leaders in leading assessments of cybersecurity programs or topics. • Provide recommendations regarding assessment scope. • Provide direction and guidance to team members on the approach to cybersecurity programmatic activities or technical performance testing. • Provide input to the Federal assessment team leaders on document requests and other necessary logistics to support the assessment team. • Provide feedback on proposed cybersecurity assessment team structure and make recommendations for allocation of resources needed to accomplish the scope. • Develop the schedule of interviews and make specific assignments. • Provide feedback to site personnel daily to validate assessment information and clearly communicate areas of concern. • Participate in briefing site management and cybersecurity personnel on assessment results, as required. • Prepare the programmatic and technical sections of the cybersecurity assessment report. • Work with the Federal team leader to resolve comments on the assessment report. • Participate in collaborative review meetings throughout the report development cycle. • Participate in pre-QRB meetings. • Participate in QRB meetings. • Deliver report for QRB per the approved targets. • Provide feedback on the overall assessment to EA-61 and EA-62 Directors. • Develop and maintain a list of programmatic topical areas required to thoroughly assess the cybersecurity programs within the Department that accounts for the latest Departmental orders and directives as well as National Institute of Standards and Technology (NIST) and Committee on National Security Systems Instruction (CNSSI) Guidance. • Develop and maintain a list of technical topical areas required to thoroughly assess the cybersecurity programs within the Department that accounts for the latest threat, vulnerability, and Departmental focus areas. • Ensure consistent assessment of all relevant topical areas in each assessment. • Ensure that technical information gathered during the assessment is delivered in the agreed-upon format and captures the necessary details to inform site POCs and management of any weaknesses or vulnerabilities discovered. • Recommend initiatives to EA-60 leadership to improve assessment capabilities. • Propose enhancements to existing infrastructure and capabilities to perform advanced research into adversaries' practices and tactics, increase understanding of advanced threats, and incorporate knowledge gained into standard assessment procedures for improved assessment results.

Role	Responsibility
Team Member(s) **Cybersecurity Specialists (Programmatic Team)** **and** **Cybersecurity Performance Testing Specialists (Technical Team)**	• Support the assessment and programmatic and/or technical team leaders in conducting assessments of cybersecurity programs or topics. • Provide input to the assessment and programmatic and/or technical team leaders on assessment scope and potential approaches for accomplishing cybersecurity assessments. • Provide input to update the assessment topical areas to include the latest Departmental orders and directives and the latest NIST and CNSSI guidance. • Conduct assessment activities following direction and guidance of the Federal assessment team leaders, and programmatic and/or technical team leaders. • Assist in preparing the schedule of interviews to accomplish during assessment activities. • Review key site cybersecurity documents prior to the assessment and provide input on missing or incomplete information to the assessment leads. • Execute external technical performance tests and capture results prior in a standard format prior to the internal testing as applicable. • Conduct thorough assessments in accordance with the assessment plan, the Federal assessment team leaders, and the programmatic and/or technical team leaders. • Validate assessment data and conclusions with site personnel daily to ensure factual accuracy. • Participate in briefing site management and cybersecurity personnel on assessment results, if requested. • Consolidate technical information obtained during external and internal portions of the assessment. • Provide written input for draft assessment reports, as directed by the Federal assessment team leader and programmatic and/or technical team leaders. • Work with the programmatic or technical leader to resolve comments on the assessment report. • Follow established assessment protocols and standards for each assessment.
Administrative Assistant	• Maintain the assessment artifacts (report, assessment plan, and review history) for all cybersecurity assessments in the approved EA repository. • Coordinate report coordination with other EA offices. • Maintain correspondence tracking system for assessment related deliverables including requests for review, report tracking, and overall assessment status. • Work with assessment teams and staff to schedule assessment related meetings including QRBs. • Maintain assessment calendars for EA distribution. • Coordinate the creation of the final report, including the appropriate transmittal memo for distribution, and provide it to the EA-60 Director. • Post the EA-60 unclassified assessment report title to Energy.gov.

Role	Responsibility
Technical Editor	• Edit assessment reports and annual FISMA reports. This includes independent editing, working closely with authors, participating in collaborative reviews, helping to adjudicate feedback from the FAR and QRB, and proofreading reports before they are submitted for approval routing. • Manage the report editorial process. • Review and edit ad hoc white papers, data calls, and reports. • Edit additional products as requested by the EA-60 team (e.g., the Assessment Process Guide, Change Control Board draft, network reauthorization packages, etc.). • Perform other duties: Additional writing, editing, or presentation development projects as assigned.

3 Collaboration with External Organizations

There is significant value in collaborating and interfacing with other DOE Headquarters program offices, field/site offices, NNSA sites, and DOE cybersecurity and information systems organizations to ensure that assessments are fully coordinated, results are clearly communicated, and identified deficiencies are adequately addressed. EA also works closely and interfaces with organizations external to DOE, such as the White House, Congress, the Intelligence Community, and NIST.

Within EA-60, the offices collaborate in the areas of scheduling, budgeting, resource forecasting, and procurement. EA-61 develops site and program information that contain valuable data points, including FISMA metrics, Federal Risk and Authorization Management Program (FedRAMP) data, threat data (Joint Cybersecurity Coordination Center [iJC3], Department of Homeland Security (DHS), open source, etc.), and POA&M data. EA-60 may consider requests from external entities such as the Insider Threat Working Group and the Privacy Office that can be scoped and appropriately tasked.

EA-60 has partnered with the DOE Office of the Chief Information Officer (OCIO) and the DHS in the assessment of the Department's high value assets (HVAs) and participates in ongoing meetings and assessments in collaboration with these stakeholders. Partnerships have also been established with other assessment organizations within DOE including NNSA, Office of Science, Office of Environmental Management, the DOE Office of the Inspector General (IG), and other DOE offices. Information shared across these entities helps inform the scheduling of assessment activities and ensures that site resources are not overburdened. Additionally, other assessment organization reports are used to inform internal assessment processes and develop a common understanding across the Department. Individuals within the office participate in the DOE Cyber and IT/OT Executive Council and DOE IMGB. EA has also established partnerships with the DOE IG, the DOE Office of the General Counsel (GC), and the OCIO, who receive copies of all EA-60 assessment reports.

3.1 Augmentee and Observer Program

EA has implemented an augmentee and observer program that includes DOE Federal or contractor subject matter experts as augmentees or observers on assessment teams.

The augmentee program allows subject matter experts from the various DOE facilities to participate in the inner workings of the assessment process and return to their home organizations with information on cybersecurity program best practices. The augmentee is considered an assessor and member of the assessment team.

The observer program offers benefits like the augmentee program; however, the observer is not involved in data collection activities and is not considered an assessor.

Requesting organizations must follow these general program concepts to ensure the integrity of the assessment process:

- The DOE/NNSA augmentee or observer is recommended in writing (emails are acceptable) by the applicable DOE Headquarters or field/site office and is selected and approved for participation by the EA-62 Director. Recommendations must come from the senior Federal manager and must include the specific objective and overall intention of the augmentee's or observer's participation.
    - Augmentees and observers will not participate in assessments at their own sites or of their program office; contractor augmentees are further restricted from participating in assessments at other sites operated by their employer or their parent organization.
    - Augmentees are fully integrated into the assessment team and participate in the data collection activities of the team to which they are assigned.
    - Observers are assigned to one or more topic teams during an assessment activity but do not conduct data collection activities.
    - In addition to approval from the EA-61 and EA-62 Directors, the assessed site/program Federal leadership must concur with the request for participation of an augmentee or observer during the assessment.

4 Assessment Types

All assessment program activities are designed to satisfy mission requirements. The assessment function is independent from DOE's line program offices (line management) in that EA-60 has no responsibility for operations, projects, programmatic activities, budget, or policy development. EA conducts multiple activities, collectively referred to as assessments, related to DOE and contractor cybersecurity program performance. Dependent upon the scope of the assessment, these activities are generally grouped into two types: announced or unannounced assessments and special assessments. Table 2 provides a list of assessment types.

Table 2: Assessment Types

Assessment Type	Description
Announced and Unannounced Assessments	• Assess the effectiveness of one or more aspects of a program's classified and/or unclassified cybersecurity program, as defined in the assessment scope. • A focused assessment can include technical testing and/or a less extensive programmatic review.

Assessment Type	Description
	• Conducted to obtain current information about operations, activities, and initiatives at a site or within a program, and may involve touring facilities, attending meetings, participating in self-assessments, or shadowing other agencies in their audit activities.
Special Assessments	• Conducted at the request of the Secretary or other senior DOE leaders, often on a "rapid response" basis, to provide specific information about a program's cybersecurity posture using realistic threat scenarios.

4.1 Assessment Activities

Cybersecurity assessment processes, procedures, and tools are continually reviewed and refined to remain current with the threats and trends in cybersecurity. EA-60, EA-61 and EA-62 apply each of these processes and tools according to the scope and scale of the assessment.

Cybersecurity assessment activities use a systematic approach that includes examination of the management, operations, and technical controls as well as technical performance testing 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 a site's cybersecurity program. Technical performance testing provides a good snapshot of the effectiveness of technical implementation but does not provide insight into the sustainability and direction of the program. Technical weaknesses that are identified through performance testing may be symptoms of larger, more pervasive problems associated with management of the cybersecurity program. Therefore, a significant emphasis is placed on complementing technical performance testing with a programmatic review to assess the effectiveness of key underlying management processes associated with cybersecurity programs. This approach results in identification of systemic issues and provides a basis for evaluating the direction and sustainability of the associated cybersecurity programs.

4.1.1 Programmatic Assessment Activities

During programmatic assessments, the assessment team evaluates the effectiveness of DOE cybersecurity policy implementation through an overall program review. This activity is usually conducted in conjunction with technical performance testing. The team provides feedback to the DOE OCIO and, as relevant, to the NNSA OCIO. The assessments also evaluate DOE program office and field/site office performance as it relates to implementation of the cybersecurity programs. Programmatic assessment activities are conducted via data gathering, analysis of program and policy documents requested through data calls, and interviews with various site-, program-, or office-specific personnel.

4.1.2 Technical Assessment Activities

4.1.2.1 Announced External Performance Testing

Performance testing is typically conducted in conjunction with an announced cybersecurity assessment. Announced activities are primarily used to provide an overall assessment of a program's external network security posture. These assessment activities are conducted from EA-60's CSTN. External performance testing may consist of:

- Scanning network systems exposed to the internet for vulnerabilities and attempting exploitation to evaluate the potential impact of weaknesses.
- Leveraging DOE OCIO external testing capabilities and leveraging their results or assisting site personnel and management with understanding the impact.

4.1.2.2 Unannounced Performance Testing

Unannounced performance testing is primarily used to evaluate a program's ability to withstand focused attacks from internal and external sources. The unannounced assessment activity may be performed using the internet, site wireless network, or internal device placement. The key aspect to unannounced assessments is that only key stakeholders and the white cell (i.e., a group of trusted agents) are informed of the assessment beforehand. The assessment leads work with the white cell to coordinate activities and to ensure that any areas of the network that should be excluded from testing activities are known to the assessment team in advance. Under no circumstances will testing occur without an approved assessment plan and coordination with DOE GC and the white cell.

4.1.2.3 Internal Performance Testing

Internal performance testing evaluates the strength of internal boundaries that provide isolation between differing need-to-know environments and determines potential areas of vulnerability among the in-place cybersecurity technical controls. Internal performance testing is typically conducted on site or remotely for announced assessments, may be applied to either classified or unclassified resources, and may include scanning site wireless networks to identify unauthorized or misconfigured wireless access that could provide an alternative route into the network. Internal performance testing may also occur remotely depending on the nature and scope of the assessment. Testing can utilize site-provided systems, EA-60 assets, or a combination of both. Personnel from the site or program provide the technical team with a logical central location from which most scanning and performance testing activities are conducted. However, some testing must be conducted from multiple points within the site's network. Internal performance testing may also be conducted in conjunction with an unannounced assessment activity. Such testing will be carefully coordinated with the trusted agents.

Internal performance testing may also include the use of site-provided information systems and user credentials. This type of testing emulates an authorized user on the network. The assessment team will use a variety of techniques to determine the overall security of the configuration of the computer system as well as complete performance testing activities using any available tools on the system. The assessment team will use the results of this testing when conducting their evaluation of the effectiveness of incident detection processes related to the insider.

4.1.2.4 Systematic Correlation and Analysis of Networks (SCAN) Program

The Systematic Correlation and Analysis of Networks (SCAN) Program primary objective is to characterize and evaluate the internet-facing DOE information system boundaries and the technologies used to implement them. SCAN integrates internally developed and commercially procured tools into a suite of capabilities to achieve this overall objective. SCAN and the EA-60 team evaluates these systems and services and identifies potential vulnerabilities that may impact the mission of DOE. Information from the SCAN Program may be used for assessment and may be shared with DOE stakeholders with the appropriate need to know.

The primary activities of the program are as follows:

- Obtain a comprehensive, integrated overview of DOE's public-facing internet presence, including active servers (host discovery) and network services (host enumeration).
- Incorporate and analyze additional external scan information, such as American Registry for Internet Numbers, Google, and Shodan, and DOE OCIO tools, to support planning for broader cyber security assessments, identification of vulnerabilities, or to respond to ad hoc requests.
- Provide a single location for comprehensive information generated by the SCAN program describing the DOE network boundaries for use in conducting independent oversight activities or responding to ad hoc requests.
- Perform critical analysis of all collected information through SCAN to support development of testing strategies and validation for cybersecurity assessments, identification of vulnerabilities, or to validate risk factors for Department.
- Brief the analysis output of the SCAN Program to assessment teams, DOE Stakeholders, or EA Leadership based on request or need; SCAN raw data may be provided for additional threat correlation or analysis.
- Maintain technical capability to quickly response to additional special-purpose scans of internet-facing DOE systems to support the response to latest vulnerabilities or other ad hoc requests.
- As part of the Closing assessment phase, SCAN Program output (i.e. results that have been analyzed, fully processed, and correlated with assessment data) is purged and is not retained.

4.1.2.5 Open-Source Information Gathering

The goal of open-source information gathering is to identify potential targets that an adversary may use for cybersecurity attacks against information systems and in phishing or other social engineering attacks against a site or the larger DOE enterprise. The data collected informs technical performance testing and evaluation of the cybersecurity program's operational security measures that prevent sensitive information from being exposed to the public.

As part of the external assessment process, the technical team may review social media and other internet sources to look for people, information regarding the physical location (e.g., blueprints, maps, photos), and potential leakage of controlled unclassified information to the public. If the technical team identifies a potential weakness, it will immediately notify the site POCs so that they can take appropriate action. The open-source information collected is bundled into the information provided to the site POCs at the end of every assessment. EA-60 does not collect or store any information on DOE personnel. This open-source information is used to provide reference material for assessment activities and for operational security awareness.

4.1.2.6 Phishing/Human Vulnerability Testing

The goal of human vulnerability testing is to test the susceptibility of personnel to phishing or other social engineering methods commonly used by DOE's adversaries. Before testing begins, EA-60 and site POCs will discuss the testing methods and agree upon the rules of engagement (ROE) defined in the assessment plan.

Human vulnerability testing is not intended to identify poor performance of specific individuals but rather to focus on improving the cybersecurity programs. Assessment leads work with the site POCs to ensure that the testing results help direct program improvements rather than consequences for any individual.

Testing will use penetration testing and other tactics used by malicious adversaries to identify potential areas of weakness in the technical controls that should prevent successful phishing or other attacks, as well as test the overall performance of the program's detection methods. During these simulated attacks, the assessment team will evaluate the overall incident response process to determine the level of resiliency to such tactics.

4.1.3 Special Assessments

EA-60 will conduct special assessments at the request of the Secretary or other senior DOE leaders, often on a "rapid response" basis, to provide specific information by testing a program's cybersecurity posture using realistic threat scenarios. The scope and scale of such activities will vary depending on the risk to the Department as well as the overall intent of senior leadership. EA-60 will work with the involved stakeholders to leverage its combined knowledge to support the assessment efforts.

4.1.4 Other Assessment Activities

As requested by DOE leadership, internal DOE organizations, or external partner organizations, EA-60 will conduct assessments or technical performance testing activities to evaluate the effectiveness of cognizant organizations' cybersecurity programs and activities. Before starting any assessment activities, the assessment team meets with stakeholders to determine the scope, duration, and develop assessment milestones. Assessment milestones and their status communicated to the white cell to track the overall process. After the scope is determined, the Federal assessment team leader assigned to the assessment/testing activity will follow the assessment phases where applicable.

5 Assessment Phases

Figure 1: Assessment Phases

All cybersecurity assessments include five major phases: initiating, planning, conducting, reporting, and closing. Although these phases are identified as separate entities, they may overlap with one another. Subsequent sections of this document describe the activities and expectations associated with each of the assessment phases.

5.1 Initiating

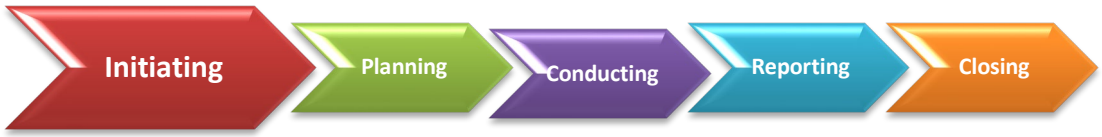

Figure 2: Initiating Phase

During the second quarter of each fiscal year, the Directors of EA-60, EA-61, and EA-62, in conjunction with EA leadership, conduct internal planning sessions to determine priorities for programs to be considered for assessments during the following calendar year. This process involves engaging stakeholders from across the DOE enterprise, evaluating mission essential functions for the Department; researching key projects and initiatives, analyzing past assessment information, evaluating requests for assessments from the program offices, and evaluating priorities presented from DOE senior leadership. Once these meetings are complete and the initial draft of the schedule is created, the EA-61 and EA-62 Directors work with the site management to factor potential schedule conflicts and develop the final dates. The EA-61 and EA-62 Directors prepare and present formal calendar year assessment schedule memos for the EA-60 Director to send to each program office and the respective sites. This process necessitates the creation of the annual cybersecurity assessment integrated schedule. This schedule identifies planning activities, key milestones, and resources required to conduct each assessment activity.

If the schedule is changed, the EA-61 and EA-62 Directors will inform the key stakeholders of the affected program office, the site, and the DOE IG.

Unannounced assessments, in most cases, can span multiple calendar years and, due to the nature of the assessment activities, are communicated to only selected individuals (i.e., white cell members) on a case-by-case basis.

Once the schedule is complete, the EA-61 and EA-62 Directors will designate Federal assessment team leaders. Support services contractor (SSC) management designates the programmatic and technical leaders. The EA-61 and EA- 62 Directors and SSC management will then initiate the development of the resource and report tracking artifacts to establish initial teams for each assessment as well as important milestone dates for reports. Projected QRB dates will also be set and used for coordination throughout the year.

5.1.1 Initiating Inputs and Outputs

Table 3 lists the inputs and table 4 lists the outputs from the Initiating phase of the assessment lifecycle.

Table 3: Initiating Inputs

Input	Resources Needed	Responsible Party	Time Frame
Past assessment information; Current priorities	Threat reports; Situational awareness artifacts; PMEF/MEF Matrix; Stakeholder request information	EA-61 and EA-62 Directors with support from the team	Available at the beginning of the Initiating phase.

Table 4: Initiating Outputs

Output	Resources Needed	Responsible Party	Time Frame/Due Date
Formal calendar year assessment memos	DOE stakeholder consensus	EA-61 and EA-62 Directors	Delivered each October and documents the activities for the next calendar year.
Assessment schedule	Final list of planned assessment programs	EA-61 and EA-62 Directors	Completed each October. Consists of scheduled activities for the next calendar year.
Site Portfolio development	Previous assessment reports	EA-61 Director	Initial list of scheduled locations established in October every year with delivery of each Site Portfolio at least 120 days prior to each assessment.
Report tracker development	Report tracker template	Administrative assistant; Logistics points of contact	Developed in October of each year for scheduled assessment activities.

5.2 Planning

Figure 3: Planning Phase

The goal of planning is to identify and prepare for the actions necessary to conduct an effective and efficient assessment of a specific site or office's cybersecurity program and to implement the management, operational, and technical controls. For different types of assessment activities, the planning phase may be tailored based on the nature and extent of the planned activity. For example, an external network security assessment that is conducted remotely from the public internet requires less planning than a full assessment.

All assessment activities are summarized in an assessment plan, developed by the assessment team leader, and approved by the EA-60 Director, EA-61 and EA-62 Directors, and site management.

5.2.1 Planning Phase Activities

The EA-61 and EA-62 Directors or the Federal assessment team leader initiates scoping and planning activities with senior Federal and contractor site management approximately 120 days prior to the assessment to solicit input for the assessment scope and to establish high-level agendas, assessment parameters, and site and assessment team points of contact. The federal assessment team leader will establish the scope of the assessment activities while also planning their execution and the follow-on phases with support from the EA-61 and EA-62 Directors and the SSC. As part of this process, the assessment leaders (Federal, programmatic, technical, and SSC management) review the assessment

team personnel and adjust the resources based on experience at the site, the site's size, and the overall scope of the assessment.

The Federal assessment leader reviews current information about the site, program, and other related threat information prior to their first contact with the program or site to be assessed. This information provides background to assist the assessment team in developing their initial scope, framing their questions, and making the most efficient use of time. The Federal assessment lead will conduct a stakeholder engagement meeting to facilitate initial introductions between the site personnel and EA team, provide a high-level overview of the EA assessment process if required, request the tailored initial data call, and request additional information about the site that will be a benefit in the initial scoping meeting. Additionally, the Federal assessment team leader will request that the site personnel prepare a mission brief, presented by site management prior to the assessment, to provide an overview of the operations and mission at the site.

Following the stakeholder engagement meeting, the assessment team will discuss the information and outcome of the meeting and set up objectives and a plan for follow up meetings with the site/program. This is also the time when scope can be refined as well as assessment strategies developed. An assessment planning meeting may be used to meet key site personnel, request additional cybersecurity program documentation, conduct exploratory interviews, or determine other priorities or concerns the sites management may have. Additional meetings may be scheduled to assist in defining the assessment strategies or logistics to successfully accomplish the objectives of the assessment and provide value back to the site or program.

Scoping and planning activities may include but are not limited to:

- Establishing assessment parameters based on research, DOE knowledge, threat information, and input from program office or site management.
- Reviewing available program information (e.g., past reports, corrective action plans).
- Reviewing site information from other EA offices to include other assessment reports.
- Identifying information systems that support key sites or program functions.
- Developing assessment objectives, focus areas, specific data requests, and tailoring the data call to get specific information needed to have a successful assessment.
- Developing assessment strategies that are unique to the site's mission, specific scope, or other concerns provided by leadership to ensure the assessment gathers the necessary data for the report.
- Identifying HVAs, as applicable.
- Coordinating logistics with site personnel, including site access issues, conference room requirements, training requirements, shipping information, and support needs.
- Coordinating logistics with site personnel for the deployment and use of remote assessment capabilities (when needed).
- Preparing an assessment plan, including preliminary identification of the assessment scope; developing preliminary programmatic assessment/review topics and interview schedules, ROE, and trusted agent forms.
- Reviewing any initial data call information provided during initial discussions with the program office or site.
- Tailoring and then requesting site documentation (data call).

- Conducting one or more planning and scoping meetings to ensure assessment objectives and strategies are well developed and achievable.
- Reviewing information provided by the site POCs in response to the team's data call request.
- Working as a team to develop and adapt to the site's specific program including working with limited documentation if required.
- Identifying potential challenges and working together to develop mitigation strategies.
- Determining training and access requirements to ensure that the assessment can start immediately on the first day.
- Shipping the assessment equipment to the site or coordinating remote access requirements to conduct the assessments from other locations.

In addition to the items noted above, unannounced assessment activities will require additional planning activities, such as the following:

- Coordination with DOE GC on the overall scope and methods to be used during the assessment.
- Coordination with the EA-60 Director regarding the overall assessment scope and communication to EA-1 Director.
- Development of key milestones for the assessment that define the delivery of updates to the white cell, delivery of information gathered to date, and the overall out brief.
- Coordination of any human vulnerability assessment activities with the white cell, EA, and DOE GC as applicable.

5.2.2 Assessment Plan

Each assessment has an assessment plan that describes the general scope and approach to conducting the assessment, defines any specific focus areas, lists team members, and establishes basic ground rules for conducting the overall assessment. In those cases where there are joint assessment activities with other EA offices, a joint assessment plan will be developed by the other office's team leader with input from the EA-60 Federal assessment team leaders. Although the assessment is not limited to evaluating the specific areas listed in the assessment plan, every effort is made to identify areas of emphasis during the assessment.

Unannounced assessments will begin with meetings with white cell representatives, where an initial scope and ROE are negotiated. Once agreed upon, the Federal assessment team leader will develop a specific assessment plan following the same process outlined above. In addition to the EA-60 and site management approvals, DOE GC and EA-1 will review the plan to ensure they have awareness and visibility in the process.

The assessment plan is sent to the site POCs and management in advance of the assessment for review and comment. In parallel, the Federal assessment team leader provides the assessment plan for approval by the EA-61 and EA-62 Directors and EA-60 Director. Once any comments are adjudicated, the Federal assessment team leader provides the assessment plan to the EA-60 Director for signature and to the DOE field/operations/site office representatives for their signature acknowledging the plan.

5.2.3 Rules of Engagement

The ROE section contained in each assessment plan outlines the respective roles and responsibilities of the assessment team, site Federal and contractor cybersecurity managers, and trusted agents for the

performance testing. The ROE explains the general approach and defines specific parameters and controls that will be followed during testing. The ROE includes the following general controls:

- Protect all information (classified and unclassified) from unauthorized access in accordance with DOE orders.
- Suspend testing at the request of the site management if there are legitimate safety, security, or operational concerns.
- Maintain frequent communications with the site POCs and management with respect to the status of testing activities, including the coordination for any additional testing of systems at other locations where IT resources are deployed.
- Provide detailed information and work with cybersecurity and/or IT personnel to return information systems to the original configuration upon completion of testing so that no systems remain in a compromised state.
- Immediately terminate testing and notify the primary and secondary points of contact of the condition in the unlikely event that performance testing adversely affects a system. Testing procedures targeting the affected system will resume only once the system state is stable and testing procedures have been modified to prevent further disruptions.
- Inform the iJC3 and/or NNSA Information Assurance Response Center (IARC) of performance testing dates to ensure that testing activities are not mistaken for real attacks.
- Obtain approval from the site Authorizing Official or Authorizing Official Designated Representative prior to any data leaving the site.
- Identify any data developed during scanning activities or data developed because of successful exploitation(s) and provide it to the site trusted agents and information system security manager.
- Provide the assessment team, through the trusted agent, with alerts or other indicators of activity that would trigger the program's incident response process, including the originating address of the event, time of day, and activity that triggered the process.

As part of establishing the ROE, the POCs are responsible for informing the assessment team when certain critical systems, such as safety systems or major business applications, are undergoing upgrades or should be excluded from testing activities. Exclusion justifications should also be provided as part of the data call. In addition, the site POCs and management must identify any system that is connected to the site network but is not under the direct control and responsibility of the program. Based on this information, the Federal assessment team leader may exclude some cybersecurity systems from performance testing activities.

5.2.4 Programmatic Data Call

The programmatic data call is broken into two parts: the initial data call and full data call. The Federal assessment team leader requests the initial data call during the stakeholder engagement meeting. The data call will be coordinated with the site POCs prior to the formal sign-off of the assessment plan to ensure all parties have adequate time to gather the assessment artifacts prior to the assessment date. The initial data call documents requested are due 30 days after the stakeholder engagement meeting, and the full data call documents are due at least 60 days prior to the assessment unless otherwise stated. If necessary, the programmatic team will convene with the cognizant site/program office POCs

and management and subject matter experts to discuss the data call and logistics for the assessment after the data call is provided. Data call document requests may include:

- Applicable local policies are used for the management of the cybersecurity program, such as local processes and procedures. Local policies may include site work instructions or procedures addressing account management, configuration management, auditing and continuous monitoring requirements, incident response, or other programs elements.
- The most recent, relevant Enterprise Cybersecurity Program Plan or site organizational and local cybersecurity protection plan(s).
- Organizational charts for the program, including cybersecurity and IT groups.
- Latest and current Security Assessment and Authorization (A&A) documentation, for example, formal Authorization to Operate (ATO) letters, security test and evaluation (ST&E) authorizations, or any granted interim authority to test letters; documentation for common control providers; system security plans; security assessment reports; ST&E results; risk assessments with residual risks; privacy impact assessments; and any other documentation/artifacts normally included with the A&A package for the program systems.
- Any program-wide cybersecurity risk assessment applicable to multiple systems.
- Any program-wide business continuity planning projects, business impact analysis documentation, contingency plan, and contingency planning documentation to identify mission essential resources, resource interdependencies, and restoration priorities.
- Latest FedRAMP security packages for any deployed cloud services, including but not limited to the ATO letters authorizing the use of the cloud service, listing of program-specific controls for the service, last 2 months of the cloud service provider continuous monitoring deliverables, and documentation of review of the cloud service provider annual assessment materials.
- List of current internal and external POA&Ms output from the DOE Enterprise Cyber Governance System and corrective action plans for the site cybersecurity program, systems, and subsystems.
- List of POA&Ms closed within the last 12 months.
- The site cybersecurity program self-assessment and third-party reports for the past 2 years and the status of corrective actions.
- The most recent FISMA Metrics report submission.
- Current methodology or plans for implementing ongoing authorization.
- Program-specific documentation for identifying critical information at the site and mission essential computing resources used to process, store, or transmit that information (equivalent to mission-critical systems). This includes the DOE HVA system list for the site.
- Program-specific threat assessment information.
- Supply chain risk management, risk assessment, plan, and lifecycle strategy.
- Date of last comprehensive program inventory of assets along with evidence or record of its completion.
- List of DOE Mission Essential Functions and Primary Mission Essential Functions that the program supports and a listing of any IT systems that support each function.

5.2.5 Technical Data Call

In addition to the programmatic data call, EA-60 will also request technical information to be delivered on the same schedule. If necessary, the technical team will convene with the cognizant site/program

office leadership and subject matter experts to discuss the data call and logistics for the assessment at least 2 weeks prior to the assessment. Technical information may include:

- All IP ranges associated with the mission, IT, and cybersecurity programs at the site, including a list of IP addresses to be excluded from testing and a detailed justification for the exclusion.
    - EA will review the exclusions along with justification and coordinate with the site personnel to determine alternative means of testing (such as special testing hours, manual scanning instead of automated scanning, etc.).
- Inventory of network endpoints.
- A network topology map containing perimeter devices and IP addresses of those devices (including the main border router and other routers that have separate internet connections), firewalls, gateways, and major subnet routers.
- Access control lists, firewall rules, and intrusion detection/prevention rules.
- The latest vulnerability scan results from the program's scanning system.
- Information related to any wireless networks in use, including service set identifier and media access control addresses of all authorized access points.

5.2.6 Logistics Information

The Federal assessment team leaders will work with the administrative assistant and the site POCs to schedule the appropriate space needed to conduct each assessment. The specific room requirements will vary depending on the size and type of assessment but in general will encompass conference room space to accommodate the following activities:

- In-brief on the first day of the assessment
- Technical testing
- Programmatic interviews
- Technical interviews
- Daily validation meetings
- End-of-day meetings for the assessment team
- Out brief

The Federal assessment team leader(s) and the administrative assistant will also request information pertaining to shipment of equipment to the site, directions to the specific buildings where the assessment will occur, and for additional meetings with senior leadership of applicable.

5.2.7 Assessment Schedule

The Federal assessment team leaders, in coordination with the programmatic and technical team leaders, will develop an initial interview schedule and provide it along with conference room and virtual communications and collaboration requirements to the program's point of contact at least 4-6 weeks prior to the assessment activity to ensure adequate space and the necessary resources are available.

The assessment schedule is designed to efficiently use time during the assessment to ensure a thorough assessment is conducted. The schedule must address the critical data collection activities needed to satisfy the scope and objectives of the assessment. Some flexibility is built into assessment schedules to allow additional interviews if unexpected or unanticipated events occur during the assessment, or to fill data gaps or clarify information. The development of the assessment schedule requires extensive

coordination with the site POCs to set up interviews, walkthroughs, tabletop reviews, and validation meetings.

The Federal assessment team leader will prepare an initial briefing for the beginning of the overall assessment. The in-brief slides will provide an overview of the assessment scope, schedule, and activities.

The assessment team will schedule daily informal validation meetings with site POCs and management to provide feedback on the progress of data collection, areas requiring further review, and issues of potential concern, if any. These meetings occur the next day, normally at the beginning of each assessment day. Additionally, a management meeting with senior site management – for example, the authorizing official and the CISO – may be held as needed to briefly discuss the progress of the programmatic review and performance testing.

Due to the nature of unannounced assessments, a milestone schedule will be developed to identify time frames when the EA-61 and EA-62 Directors or Federal assessment team leader will brief the program POCs and management white cell and other stakeholders on the status of the overall assessment, current observations, and any changes to the overall scope or planned activities.

5.2.8 Planning Inputs and Outputs

Outputs from the Initiating phase are considered Inputs for the Planning phase. Table 5 captures the additional inputs that occur within the Planning phase itself. Table 6 lists the outputs from the Planning phase of the assessment lifecycle.

Table 5: Planning Inputs

Input	Resources Needed	Responsible Party	Time Frame
Assessment planning meeting	Federal assessment team leader, technical and programmatic leaders, and site/program office stakeholders	Federal assessment team leader	50 days prior to the assessment
Coordinate Program Mission Brief	N/A	Federal assessment team leader	50 days prior to the assessment
Completed data call request to EA-60	Feedback from the site POCs; Data call delivery method	Federal assessment team leader	60 days prior to the assessment

Table 6: Planning Outputs

Output	Resources Needed	Responsible Party	Time Frame/Due Date to/from Site
Assessment planning meeting slides and meeting agenda	Slide template	Federal assessment team leader(s)	8 weeks prior to the assessment

Output	Resources Needed	Responsible Party	Time Frame/Due Date to/from Site
Completed assessment interview schedule sent to team and site POCs	Information garnered from data calls; Inputs from the assessment planning meeting and follow-up discussions	Federal assessment team leader(s); Programmatic and technical team leaders	4 weeks prior to the assessment
Conference room logistics request sent to site POCs	Assessment schedule; Room requirements; assessment planning meeting results	Federal assessment team leader(s)	6 weeks prior to the assessment
Assessment plan (to include site POCs and ROE)	Assessment plan template; document request template	Federal assessment team leaders	4–6 weeks prior to the assessment
Data call request provided to site POCs	Data call template	Federal assessment team leader(s)	120 days prior to the assessment
Logistics and travel plans	Concur; travel coordination spreadsheet	EA-61 and EA- 62 Directors; Federal assessment team leaders; Administrative assistant	4 weeks prior to the assessment
iJC3 and NNSA IARC notification (for external assessments)	iJC3/IARC notification email template	Federal assessment team leaders	5 weeks prior to the assessment
Completed site-required training and application for physical/logical access	Site-supplied forms and training materials/ instructions	Federal assessment team leader(s); Programmatic and technical team leaders; Programmatic team; Technical team	3 weeks prior to the assessment
Visitor requests submitted and accepted by site POCs	Site visitor request forms; training certificates	Federal assessment team leaders; Administrative assistant; Site POC	3 weeks prior to the assessment
Trusted agent/technical team planning meeting	Information garnered from data calls	Federal assessment team leaders; Programmatic and technical team leaders	1-2 weeks prior to assessment

Output	Resources Needed	Responsible Party	Time Frame/Due Date to/from Site
Assessment equipment setup and shipping preparation	Standard technical image; Assessment hardware; Special requests from team	Technical team leaders; Laboratory administrator	At least 2 weeks prior to the assessment
Assessment equipment sent to site	Assessment equipment; Inventory checklist; Shipping crates	Federal assessment team leader(s); Administrative assistant; Technical team leaders; Laboratory administrator	1 week prior to the assessment
Final in-brief slides sent to team and site POCs	In-brief/ briefing template	Federal assessment team leaders	1 week prior to the assessment

5.3 Conducting

Figure 4: Conducting Phase

The goal during the Conducting phase is to collect sufficient information regarding the performance, direction, and sustainability of classified and unclassified cybersecurity programs. During the Conducting phase of the assessment, the assessment team conducts performance testing and performs a programmatic review to evaluate whether the documented process is indeed achieving the desired outcome through review or artifacts, dashboards, and interview feedback. This phase may include activities such as external assessment results, interviews, walkthroughs, tabletop reviews, and data analysis that are customized to accurately assess the program's ability to protect its classified and unclassified information. During this stage, the team develops assessment conclusions based on analysis of data and validates information with site personnel.

To gain insight into a site's cybersecurity programs and to understand interdependencies with other site activities, the assessment uses a "bottom-up" approach to program assessment. As a first step, unclassified cybersecurity assessments will begin with extensive external network performance testing. This performance testing, including attempts to penetrate the site's network, is conducted remotely over the internet using DOE-authorized information systems. The technical team will also conduct performance testing internally to validate the processes in place to minimize and/or mitigate the

impacts of an insider. The technical team may also conduct tabletop reviews of information systems excluding performance testing, firewall rules, and intrusion detection systems to fully assess the implementation of the security controls. The assessment activities will vary depending on the specific site or program being assessed and are tailored to best align with adversary techniques. As noted in the Planning section, the assessment team leaders will review any request and justification for exclusion of certain critical safety or operational systems from testing to determine the proper testing activities.

Unannounced assessments follow a similar format, but there is no in-person assessment scheduled, and the full timeline may be months or multiple calendar years in duration. The assessment activities will vary depending on the specific program being assessed and are tailored to best align with adversary techniques. The assessment plan and ROE will outline any specific or prohibited activities and will be discussed with the white cell before the assessment begins.

5.3.1 Technical Approach

The approach to the technical assessment, also referred to as performance testing activities, is a key element of cybersecurity assessments because it provides tangible feedback on the current effectiveness of a program's ability to protect and defend the information systems. Performance testing is based on in depth knowledge of the current threat environment, attack and exploitation methods and techniques used by adversaries, and known vulnerabilities associated with various network designs, operating systems, and application software. The technical teams will use tactics employed by malicious insiders to gain access to the program's information systems to evaluate the program's ability to detect and deter the insider threat. These tests will evaluate the effectiveness of implemented controls and identify potential weaknesses. Technical team members plan and conduct performance testing based on this knowledge and the characteristics of the program resources.

The technical team may also use site-provided computer systems and user credentials to emulate a trusted insider and/or a computer system compromised by an external attacker on the site's network. During this process, the technical team can determine whether locally available tools or other techniques might expose weaknesses with current configurations. In conjunction with this testing, the technical team will also review the testing procedures and results with the program's incident responders to determine whether there are opportunities to improve the program's detection and response processes or augment existing capabilities. Although initial targets and testing objectives may be established prior to performance testing, the technical team may deviate from those initial targets and objectives if preliminary test results indicate unknown or unanticipated systems, results, or activity.

Performance testing comprises vulnerability scanning and exploitation of identified vulnerabilities. In addition, the technical team will test web applications and databases for vulnerabilities that may be the result of misconfigurations and not readily identified through vulnerability scanning. The technical team may also perform testing of information systems used for control systems, operational technology, Supervisory Control and Data Acquisitions, critical safety systems, or Internet of Things devices to determine whether weaknesses exist that could pose a risk to the site's mission or to personnel. Cybersecurity assessments also include searches for wireless access points controlled by the program that may be vulnerable and allow access into the site's network. The exploitation of vulnerabilities is performed to determine the impact to the enterprise and the detection and response capabilities of the program and is conducted in coordination with the trusted agent. If egregious vulnerabilities are

identified, testing is halted, and the site POCs and management are informed of the vulnerability and given the opportunity to provide remediation or mitigation.

However, performance testing by itself does not allow for valid conclusions on the direction or sustainability of the program. Technical interviews are conducted to assess the effectiveness and stability of the program and to evaluate essential operational processes that form the technical implementation of the cybersecurity program. Performance testing and interview results are also used as input for the programmatic review to determine specific weaknesses (symptoms) and identify root causes of systemic problems. The combination of extensive performance testing and review of essential program elements allows the assessment team to fully and effectively assess unclassified and classified cybersecurity programs.

Unannounced assessments follow a similar structure to announced assessments and use many of the same techniques and leverage the same expertise to attempt to compromise the program information systems. The primary difference between these and announced activities is that the assessment team works as if it is an external adversary attempting to gain access. When warranted, the team will also work with the white cell to pose as a malicious insider to test the effectiveness of the in-place security controls as part of the overall assessment. Unannounced assessments do not follow the same interview process as announced assessments; however, additional interviews with site personnel may be conducted after performance testing to understand more about the response actions taken or why a particular test was successful or not successful. All these activities will be scheduled and coordinated as part of the ongoing assessment process.

Any misuse of information systems detected during performance testing is reported immediately to site management. If criminal activity is suspected, the Federal assessment team leaders report this information to the EA-61, EA-62, and EA-60 Directors who convey that information to the DOE IG for investigation and resolution. EA-60 does not investigate alleged criminal activity or misconduct. The site personnel are responsible for reporting computer security incidents to program officials, iJC3, IARC, and other organizations, as appropriate. The Federal assessment team leaders are responsible for coordinating the performance testing activities with iJC3 and the NNSA IARC.

5.3.1.1 Trusted Agents

The cooperation and assistance of DOE site representatives is essential to ensure a full and accurate cybersecurity assessment. The trusted agents provide detailed site and systems knowledge, arrange administrative and logistical support, expedite assessment activities, and provide valuable feedback on factual accuracy.

Collaboration between the assessment team and local representatives must be open and professional to provide maximum value. This collaborative approach is especially important during performance testing, where trusted agents are used to maximize realism while maintaining the confidentiality of the scenario or test content and the timing of scheduled, limited-notice, and no-notice tests. All trusted agents sign a Trusted Agent Roles and Responsibilities Acknowledgement form prior to being briefed on sensitive test information. Finally, the assessment team shares performance test materials with trusted agents in person or, when necessary, by encrypted email. These materials should not be forwarded to anyone who does not have a need to know.

5.3.2 Programmatic Approach

The programmatic team conducts interviews with Federal and contractor cybersecurity and IT personnel, reviews new or revised documentation not submitted with the data call, confirms cybersecurity program elements demonstrated by site personnel (e.g., online training material, configuration management records, issue reporting and tracking systems), and coordinates the results of these activities with members of the technical team to either confirm that program performance is consistent with program policies or to identify elements where performance deviates from policies and standards. The programmatic team, in coordination with the Federal assessment lead, will specifically examine the program's insider threat risk assessment processes and how the program uses the results to identify and implement controls to mitigate the risk to an acceptable level. The team may conduct additional reviews to determine how the program addresses the specific security controls used to detect and/or deter a malicious insider, as required by the Department, NIST, and CNSSI.

Assessment team members gain an understanding of program-specific details of each evaluation element through interviews, document reviews, and performance testing and analyze these details and assess how the components are integrated to maintain an effective cybersecurity posture. Assessment team members may collect additional data as needed to determine the reason(s) for any initial indications of incomplete program implementation or inadequate technical controls. These activities may reveal documentation or decisions made regarding program and technical control implementation that were not previously provided, or local directives and decisions that specified the current program implementation of program or technical controls. Part of the assessment process involves determining whether site personnel are aware of the status of existing programmatic and technical controls or whether any identified deficiencies were not known by site personnel prior to the assessment team visit. The program review also encompasses extensive communication with site management and staff to ensure that facts and issues are accurately characterized.

Unannounced assessments may include elements of the programmatic review at the conclusion of the technical testing to identify systemic issues within the program that contributed to any weaknesses identified.

5.3.3 Communication and Feedback

The objective throughout each assessment activity is to ensure that a thorough and accurate assessment of the cybersecurity program is conducted, and that management gain maximum benefit from the experience. To accomplish this, the assessment team, site managers, and cybersecurity staff must all communicate effectively. This communication begins prior to the assessment activities and continues throughout the assessment lifecycle. Initial communication begins with the initiating and planning process and the development of the assessment plan and ROE and continues during the assessment activities, beginning with an in-brief to site personnel that covers the scope, interview schedule, and report preparation process. Following these high-level briefings, the programmatic and technical teams meet with their respective site POC to begin the assessment activities.

During both performance testing and programmatic reviews, the assessment team will provide routine feedback to the site POC and management on the progress of the assessment, keeping site personnel informed of any potential concern associated with the review. This exchange occurs during daily validation meetings, normally starting on the second day of the assessment. These meetings summarize

the previous day's activities, and any observations related to the assessment, and allow the assessment team leaders to ask any follow-up or validation questions. The site POC and management has an opportunity and responsibility to provide feedback or concerns about factual accuracy. The site POC and management should provide additional data and identify site personnel who can help identify corrections for any factual accuracy misunderstanding. The activities listed in section 5.3.4 are integrated into the assessment process to ensure that the assessment team and site managers and staff have an opportunity to effectively communicate. If necessary, the Federal assessment team leaders will hold supplementary meetings with the site or field office Federal staff or management regarding key observations as applicable.

At the conclusion of an assessment, the Federal assessment team leaders present the pre-decisional results of the assessment to the key DOE field/site and contractor line managers, highlighting program strengths, any identified weaknesses, and areas for improvement related to the program's classified and unclassified cybersecurity programs. The pre-decisional closeout briefing will focus on a description of the strengths and weaknesses of the program and conclusions developed by the assessment team. Specific findings may also be discussed due to the severity of such weaknesses.

Communication for unannounced assessments will follow the established reporting timeline developed as part of the planning phase. EA-60 will inform the white cell and other stakeholders as negotiated during the planning process on the status of activities, any observations identified, and the plan for any new or upcoming assessment activities. These reporting sessions may also identify new areas to assess, and the Federal assessment lead will work with the white cell for approval if necessary. If at any time during the assessments the team determines that the program is at risk of attack based on an identified vulnerability, the Federal assessment team leaders will immediately notify the program of the issue so that the program POCs and management can take appropriate action.

Periodically, sites ask for feedback on their approach to implementing cybersecurity measures or request recommendations regarding products. As part of its effort to assist DOE sites and programs, the assessment team is open to conducting a dialogue on technical issues. As an assessment organization, EA-60 does not direct a program to take any specific action, use any specific cybersecurity tools, or adopt any specific technical solutions. Rather, the assessment team will engage in technical dialogue to provide feedback on the advantages and disadvantages of specific applications, approaches, and implementation. Selection of applications, approaches, and implementation remains a line management responsibility.

5.3.4 Testing Conclusion Activities

At the conclusion of each assessment, the Federal assessment team leaders are responsible for the following:

- Notifying iJC3 and the NNSA IARC that testing activities are complete.
- Conduct a hotwash with members of the assessment team to gather lessons learned.
- Providing overall direction for the report to programmatic and technical assessment team leaders including but not limited to specific issues to be called out in the report and their context.

- Ensuring that the assessment results describe the performance for the overall program including any specific areas of focus or follow-up items as defined during the initiating and planning phases.
- Developing a written summary of the assessment observations and results and delivering it to the EA-60 Director and EA-61 and 62 Directors.
- Conducting post-assessment briefings with senior program office or EA officials related to assessment activities as requested.

5.3.5 Conducting Outputs

Outputs from the Planning phase are considered inputs to the Conducting phase. Table 7 lists the outputs from the Conducting phase of the assessment lifecycle.

Table 7: Conducting Outputs

Output	Resources Needed	Responsible Party	Time Frame/Due Date
Commence external testing of the site-provided IP ranges	Scanning hardware and software; Program data call	Technical assessment leader; Technical assessment team	4 weeks prior to the assessment
Consolidate external assessment data for delivery to site	Scanning results; Open-source information	Technical assessment leader	1 week prior to the assessment
Consolidate assessment data for delivery to site	Internal and external scanning results	Technical assessment leader	End of the assessment
Daily validation meetings	Daily input from the programmatic and/or technical team	Federal assessment team leaders; Programmatic and technical team leaders	Daily during assessment activities
Pre-decisional closeout briefing	Consolidated daily input from the programmatic and/or technical team	Federal assessment team leaders; Programmatic and technical team leaders	End of the assessment
Notify iJC3 and the NNSA IARC of testing completion	iJC3/NNSA IARC closeout email template	Federal assessment team leader(s)	First day of return from the assessment
Assessment hotwash	Assessment hotwash	Federal assessment team leader(s)	First week after return from the assessment
Develop written summary	Written summary objectives	Federal assessment team leader(s)	4 days after return from the assessment

5.4 Reporting

Figure 5: Reporting Phase

At the conclusion of each assessment, a report is issued to formally document the results of assessment activities and is intended for dissemination to the Secretary, appropriate DOE managers at DOE Headquarters and in the field, and site contractors. The results of EA-60 assessments may include deficiencies, which in accordance with DOE Order 227.1A, Chg. 1, *Independent Oversight Program*, represent inadequacies in the implementation of an applicable requirement or performance standard. EA-60 assessments may also identify findings, which are deficiencies that warrant a high level of management attention and that, if left uncorrected, could adversely affect the DOE mission, worker safety and health, the public, or national security. EA-60 may also provide OFIs, which are included to assist line managers in improving programs and operations. Although OFIs may identify potential solutions to findings and deficiencies identified in EA-60 reports, they may also address other conditions observed during the assessment process. OFIs are provided only as recommendations for line management consideration. Finally, EA-60 assessments may identify best practices, which are safety- or security-related practices, techniques, processes, or program attributes observed during an assessment that may merit consideration by other DOE and contractor organizations for implementation.

The goal of the Reporting phase is to thoroughly analyze all available data and draw valid conclusions to prepare an assessment report and inform site management of the results. The Federal assessment lead is responsible for sending the report to EA-1 for concurrence within 60 days of completion of assessment activities.

5.4.1 Analysis of Results

Although analysis is an ongoing process during all phases of an assessment, it culminates during the reporting phase. Analysis involves the critical review of all available information from the assessment to identify specific strengths and weaknesses of a cybersecurity program, as well as underlying root causes for a condition of concern. The goal of analysis is to develop logical, supportable conclusions that portray an accurate picture of how well a cybersecurity program functions to protect classified and unclassified DOE information systems. These conclusions should take into the account the mission, priorities, and other information related to the site or program assessed to provide valuable information to assist management in reducing risk and increasing overall cybersecurity.

Weaknesses are analyzed both individually and collectively; they are balanced against strengths and mitigating factors to estimate their overall impact on performance. Weaknesses also take into consideration controls that are relaxed during assessment activities, where weaknesses are found, and the overall impact to the sites core mission functions. This analysis may lead to identification of deficiencies that cause specific weaknesses. Factors that are considered during analysis of weaknesses include:

- Importance or significance of the weakness.
- Compensating controls are implemented within the information system.
- 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.
- Actual or potential effect on mission performance or accomplishment.
- Relevant DOE policy.

5.4.2 Report Preparation

The cybersecurity assessment report is prepared following the report format and report schedule. The programmatic and technical team leaders, in coordination with the Federal assessment team leader(s), are responsible for preparing the draft assessment report. The designated lead writer has responsibility for the overall report and assigns responsibility for writing various programmatic and/or technical sections of the report to the other assessment team members.

EA-60 develops unclassified reports whenever possible. If there are any questions regarding the classification of a planned section or result, the team members will consult an EA-62 authorized derivative classifier *prior to* writing. If the decision is that the intended content could be classified, that portion of the report must be written on an appropriately authorized classified system as an addendum or supplement to the main report.

Although reports may vary in format due to differences in assessment scope, report preparation activities share a common process:

- The team prepares the initial draft report consistent with the data collected and information that has been validated during the Initiating, Planning, and Conducting phases of the assessment.
- The respective team leader and assessment team personnel review the draft report prior to the formal editorial process.
- EA-60 management reviews the initial draft report for messaging, completeness, and quality.
- The Federal assessment team leaders provide the report to the site POC and management for FAR.
- The QRB reviews the draft report to ensure that it is readable, logical, and contains adequate, balanced information to support the conclusions.

5.4.3 Collaborative Review Meetings

During the report development phase, the EA-61 and EA-62 Directors and Federal assessment team leaders will work in conjunction with the SSC management to conduct a review of the initial draft of the report. This initial review ensures that the report is accurate and contains the necessary information to support the conclusions and observations presented in the report. The technical editors will finalize the document and remove the comments and edits for the next phase of the process.

5.4.4 Draft Report Distribution for Factual Accuracy Review

The technical editors provide a new copy of the report to the Federal assessment team leader(s), who create and provide a comments resolution matrix to the site POCs and management along with the initial draft report. The site POCs and management uses the matrix document to identify specific sections of the report where there are factual accuracy comments. Formal factual accuracy comments from the site are requested within 5 working days after receiving the draft report. Reports associated with the assessments of FIEs are also provided to the DOE Headquarters IN Cyber Directorate for factual accuracy comments during this same five-working-day period.

The assessment team leaders review all factual accuracy comments and make changes to the report, as appropriate. FARs are not intended to allow site POCs and management to eliminate conclusions or findings that the site POCs or managers view as unfavorable, nor are the FARs intended to allow the site POCs and management to provide progress reports or changes in status that occurred since the assessment was conducted. The assessments are designated as a "snapshot in time," and the assessment reports document the conditions in effect at that time. Follow-on interviews or documentation reviews may be required to validate the information provided.

The Federal assessment team leaders, lead writer, and specific assessment team members will work to adjudicate the comments to develop the next version of the report and provide it to the technical editors for final update. Once complete, the report is sent back to the EA-61 and EA-62 Directors and Federal assessment team leaders for the QRB.

5.4.5 Pre-QRB Collaborative Review

The newly updated report from the FAR is provided to the QRB members for their comments. Once collected, the Federal assessment team leaders will hold a pre-QRB collaborative review meeting to discuss the comments and determine a team response or corrective action. This meeting is chaired by the Federal assessment team lead. Once complete, the Federal assessment lead provides the report back to the QRB members prior to the QRB meeting.

5.4.6 Quality Review Board

The QRB serves as a valuable tool for EA to ensure clarity, accuracy, appropriate tone and messaging, and consistency in EA written reports. The requirements and roles and responsibilities are documented in the EA Quality Review Boards Business Policy. The QRB is chaired by the EA-60 Director and includes senior personnel from other EA offices; the EA-1 Deputy Director serves as Advisor to the QRB.

5.4.7 Finalizing the Report

Once all comments have been adjudicated and the report is formatted, the Federal assessment team leaders will develop a transmittal memo and assessment summary document to the administrative assistant to route for approval by the EA-60 Director and then for EA-1 concurrence. The report is then sent to the program office for coordination prior to the final briefing of the report to the Office of the Secretary. Once all coordination is complete, the EA-60 Director distributes the final report via email and then uploaded by the administrative assistant to the EA document repository for archival purposes.

5.4.8 Reporting Outputs

Outputs from the Conducting phase are considered inputs to the Reporting phase. For each iteration of the draft report, inputs in the form of comments and edits are provided by the party responsible. Table 8 lists the outputs from the Reporting phase of the assessment lifecycle.

Table 8: Reporting Outputs

Output	Resources Needed	Responsible Party	Time Frame/Due Date
Report input from programmatic and technical team members to feed into the draft assessment report	Analytical data gathered during the assessment activities	Lead writer; Assessment team members assigned writing duties	5 days after the conclusion of the assessment
Draft assessment report for management review	Input from the assessment team members; Analytical data gathered during the assessment activities	Federal assessment team leaders; Lead writer; Assessment team members assigned writing duties; Technical editor	25–30 days after the conclusion of the assessment
Draft assessment report with management review comments	Draft report for management review	EA-61 and EA-62 Directors; Federal assessment team leaders; SSC senior management	2 days after receipt of draft report for management review
Federal lead provides draft report to site POCs and management for FAR	Updated draft report with management review comments; Adjudicated comment matrix	Federal assessment team leaders	Report sent 1 day after receipt of draft report
Site POCs returns FAR comments	Comment matrix	Site personnel	Approximately 35 days after the conclusion of the assessment
Address FAR comments and submit draft report for final formatting and editing	Site-completed comment matrix	EA-61 and EA-62 Directors; Federal assessment team leaders; Lead writer; Assessment team members assigned writing duties; Technical editors	2 days after receipt of draft report from site POCs and managers
Complete technical editing and final formatting and submit draft report for QRB review	Updated draft report based on FAR comments with final formatting	Technical editors Lead writer	6 days after receipt of draft report

Output	Resources Needed	Responsible Party	Time Frame/Due Date
Federal assessment team leader submits to administrative assistant for distribution to QRB	Final formatted draft report	Federal assessment team leaders; Administrative assistant	1 day after receipt of final formatted draft report
QRB review	Final formatted report	QRB members	5 days
Conduct QRB and generate updated draft report	Final formatted draft report with adjudicated QRB comments	QRB members; EA-60 Director; EA-61 and EA-62 Directors; Federal assessment team leaders; Lead writer; Assessment team members assigned writing duties; Technical editors	Approximately 52 days after the conclusion of the assessment; scheduled and coordinated after initial assessment schedule is developed
Final assessment report generated based on finalized report from QRB	Updated draft report from QRB review	EA-61 and EA-62 Directors; Federal assessment team leaders; Lead writer; Assessment team members assigned writing duties; Technical editors	Approximately 58 days after the conclusion of the assessment
Transmittal memo and assessment summary	Final assessment report; Memo distribution list	Federal assessment team leaders	58 days after the conclusion of the assessment
EA-1 Approval of Report	Final assessment report	Federal assessment team leader, administrative assistant	60 days after the conclusion of the assessment
Program Office Coordination and Assessment Briefing	Final assessment report; Assessment report summary	EA Office of Resource Management	65-90 days after the conclusion of the assessment.
Notification to EA-61 of final report distribution	Review and approval ticket	Administrative assistant	Automatic notification sent once review and approval ticket is closed

5.5 Closing

Figure 6: Closing Phase

The Closing phase includes all the activities necessary for the assessment team leader to close the assessment. Lessons learned during the assessment are captured, and information is properly archived. This phase marks the end of the assessment process.

5.5.1 Process Improvement

EA-60 supports the concept of continuous improvement to make cybersecurity assessments more effective and of value to DOE sites, Departmental managers, and other stakeholders. EA-61 and EA-62 Directors are responsible for soliciting feedback from each team member and making process improvement recommendations.

The EA-61 and EA-62 Directors also solicit feedback from DOE field and contractor line managers to ensure that the assessment process provides value to site personnel and welcomes any feedback on how assessment processes can be improved.

5.5.2 Documentation of Assessment Activities

The assessment team members collect a large volume of data and information through performance testing, document reviews, and interviews. The assessment processes are designed to assure the factual accuracy of information presented in assessment reports. This documentation of results is necessary to fulfill EA-60's mission of conducting the annual evaluation of DOE classified IT systems and providing input to the annual FISMA reports, as required by DOE Orders 227.1A, Chg. 1, 226.1B, and 205.1D. Each member of an assessment team has a role in documenting assessment activities for use in developing conclusions. The EA-61 and EA-62 Directors are responsible for ensuring that key assessment information is captured and retained in formal documentation.

EA-60 will not retain large volumes of information to document assessment activities. All security requirements for the marking and handling of classified documents will be strictly followed for any information retained as part of an assessment. All assessment documentation that is retained will be for internal use only, except as authorized by the EA-61 and 62 Directors in support of the annual IG FISMA report development.

Data calls, technical data, or other supporting documentation created by the assessment team during the assessment process will be deleted within 15 days of report distribution.

5.5.3 Records Retention

EA-60 maintains copies of the following documents in the EA document repository for each assessment activity.

- Signed assessment plan
- Factual accuracy review comments matrix
- Final report, with transmittal memo

5.5.4 Closing Outputs

Outputs from the Reporting phase are considered inputs to the Closing phase. Table 9 lists the outputs from the Closing phase of the assessment lifecycle.

Table 9: Closing Outputs

Output	Resources Needed	Responsible Party	Time Frame/Due Date
Finalize copies of documents listed in section 5.5.3	EA document repository	Administrative assistant; Federal assessment team leaders	Occurs automatically after review and approval action is closed, no more than 7 days after report distribution
Purge assessment data	Access to shared repositories	Federal assessment team leaders; Programmatic and technical team leaders	15 days after report distribution
Update Assessment Tracking Repository	Final report; Assessment team feedback	EA-61	30 days after report distribution

Appendix A: Definitions

Assessments – An assessment, either announced or unannounced, is an independent oversight activity conducted by the Office of Enterprise Assessments (EA) to evaluate the effectiveness of line management performance and risk management and/or the adequacy of Department of Energy (DOE) policies and requirements.

Best Practice – A best practice is a safety- or security-related practice, technique, process, or program attribute observed during an assessment that may merit consideration by other DOE and contractor organizations for implementation because it: (1) has been demonstrated to substantially improve safety or security performance of a DOE operation, (2) represents or contributes to superior performance (beyond compliance), (3) solves a problem or reduces the risk of a condition or practice that affects multiple DOE sites or programs, or (4) provides an innovative approach or method to improve effectiveness or efficiency.

Cognizant Manager – The cognizant manager is the DOE field or Headquarters manager who is directly responsible for program management and direction, and the development and implementation of corrective actions. Cognizant managers may be line managers or managers of support organizations.

Deficiency – A deficiency is an inadequacy in the implementation of an applicable requirement or performance standard that is found during an appraisal. Deficiencies may serve as the basis for one or more findings. In accordance with DOE Order 227.1A, Chg. 1, *Independent Oversight Program*, EA may use site- or program-specific equivalent nomenclature when assigning deficiencies and findings.

Directives – Directives are defined in DOE Order 251.1D, Chg. 1, *Departmental Directives Program*.

Factual Accuracy – Factual accuracy is the process by which EA validates the accuracy of collected data at the time of the assessment and ensures that identified deficiencies and their impacts are effectively communicated to responsible managers and organizations.

Findings – Findings are deficiencies that warrant a high level of attention on the part of management. If left uncorrected, findings could adversely affect the DOE mission, the environment, worker safety or health, the public, or national security. Findings define the specific nature of the deficiency, whether it is localized or indicative of a systemic problem and identify the organization responsible for corrective actions.

Opportunities for Improvement – Opportunities for improvement (OFIs) are suggestions offered in EA assessment reports that may assist cognizant managers in improving programs and operations. While they may identify potential solutions to findings and deficiencies identified in assessment reports, they may also address other conditions observed during the assessment process. OFIs are provided only as recommendations for line management consideration; they do not require formal resolution by management through a corrective action process. These potential enhancements are not meant to be prescriptive. Rather, the responsible line managers should determine their applicability based on system configuration and appropriate risk management considerations. These recommendations may

be prioritized and modified, as appropriate, in accordance with specific programmatic and information security objectives.

Penetration Testing – Penetration testing is a specific set of "Performance Testing" activities including but not limited to vulnerability scanning, exploitation of vulnerabilities and/or weak configurations, automated or manual web application testing, and other testing activities designed to evaluate the technical security controls implemented by DOE sites and organizations. Penetration testing activities may also be designed specifically to test incident detection and response capabilities.

Performance Testing – Performance testing is the conduct of activities to evaluate all or selected portions of systems, networks, or programs as they exist at the time of the test. Performance testing includes, but is not limited to, tabletop exercises, penetration testing, continuous automated scanning, and vulnerability scanning. Performance testing can be conducted as part of an announced or unannounced assessment activity.

Trusted Agent – A trusted agent is an individual with appropriate operational authority or who has a compartmented role for coordination and conduct of EA's scheduled, unannounced, limited-notice, and no-notice performance test activities. Trusted agents are responsible for maintaining strict confidentiality of performance testing information in the interest of test validity. Trusted agents must remain impartial in validating and developing performance test parameters and events necessary to evaluate identified objectives. Due diligence must be applied to limit the number of trusted agents to the minimum needed to effectively conduct the test.

White Cell – A white cell is a group of trusted agents composed of members of the site's management who are aware of the unannounced testing and will maintain the confidentiality of all assessment activities unless a situation warrants further communication to the site personnel. This white cell serves as the primary communication conduit for all activities and will be used for deconfliction if unannounced assessment activities are discovered. The white cell will also provide EA with any specific exclusion parameters to be used during unannounced testing activities.