U.S. DEPARTMENT OF
ENERGY

EA Enterprise Assessments

Office of Cyber Assessments

Assessment Process Guide

December 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.
1.6	EA-60, EA-61	August 2025	Removing redundant sections and clarifying focus. Add threat specialist role.
2.0	EA-60	October - December 2025	Post EA-60 restructuring, removing 61 and 62 references; updating to focus on this as a guide, not procedure.

Office of Cyber Assessments
Assessment Process Guide

Approval Form

Approved by: CHRISTOPHER MCFEARIN

Digitally signed by CHRISTOPHER MCFEARIN
Date: 2025.12.18 13:09:41 -07'00'

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

Table of Contents

Acronyms

CISO	Chief Information Security Officer
CNSSI	Committee on National Security Systems Instruction
DHS	Department of Homeland Security
DOE	U.S. Department of Energy
EA	Office of Enterprise Assessments
EA-60	Office of Cyber Assessments
FAR	Factual Accuracy Review
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
IN	Office of Intelligence and Counterintelligence
IT	Information Technology
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
OCIO	Office of the Chief Information Officer
OFI	Opportunity for Improvement
OSIG	Open-source Information Gathering
QRB	Quality Review Board
ROE	Rules of Engagement
SCAN	Systematic Correlation and Analysis of Networks
SSC	Support Services Contractor

1 Introduction

This Assessment Process Guide describes Department of Energy's (DOE) Office of Enterprise Assessments (EA) Office of Cyber Assessments (EA-60) techniques and procedures for evaluating the effectiveness of DOE cybersecurity programs, including the National Nuclear Security Administration (NNSA), the Power Marketing Administration, and contractor organizations' protection of special nuclear material, classified information, and controlled unclassified information.

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 of EA-60.

This Assessment Process Guide is part of an ongoing effort to maintain the quality and consistency 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-60 Federal staff and/or Director for consideration.

This process guide applies to EA-60 Federal and Contractor 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 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, either onsite or remote.
- 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 (OSIG) 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 assessment 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 Departmental working groups to maintain situational awareness and provide subject matter expertise, including, but not limited to:
    - Cyber and Information/Operational Technology Executive Council
    - DOE Information Management Governance Board
    - DOE Insider Threat Working Group
    - DOE Enterprise Architecture Governance Board
    - Chief Information Security Officer (CISO) Roundtable.

Applicable DOE orders related to the overall assessment process can be found in the *Office of Cyber Assessments Program Plan*.

2 Organization

The EA-60 Director oversees and monitors the operations of the office. The Director also maintains situational awareness of key Department priorities and gathers feedback on EA-60 assessments to improve the overall value of the assessment results, improve capabilities, and to enhance the cybersecurity posture of DOE. The EA-60 Federal staff and support service contractor work alongside one another to plan, conduct, and effectively report on the results from each unique, threat-informed assessment.

2.1 Roles and Responsibilities

Each member of the assessment team is an integral part of the assessment life cycle. Each team member may fulfill one or multiple responsibilities during an assessment. These responsibilities are largely completed remotely during the pre- and post-assessment activities (see section 5). Whether these responsibilities are completed in person or on site is determined by the overall needs of the assessment and resource availability.

2.1.1 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.
- Provide overall office direction and goals for the assessment process.
- Participate in DOE and other agency working groups to gather additional information for input into the assessment process.
- Ensure Federal and contractor collaboration and support that enable successful completion of assessment goals and objectives.

- Ensure that the Federal staff and support service contractors are effectively researching and analyzing new Federal requirements, DOE directives, policy, and other official guidance to make recommendations for inclusion into the assessment process.
- Empower Federal staff to work alongside cognizant DOE line managers and policy organizations to resolve disagreements on assessment schedules, results, findings, deficiencies, or opportunities for improvement (OFIs).
- Provide coordination, coaching, and oversight of Federal staff in the conduct of assessments, leadership, and stakeholder engagement.

2.1.2 Threat Specialist and Threat Liaison

- Research adversaries, vulnerabilities, and emerging threats related to DOE and its mission and share knowledge in staff meetings, team meetings, and learning sessions.
- Assess the potential impact of threats to programs, mission, and assets related to specific cyber assessments or DOE mission areas and suggest potential targets for new assessments.
- Create tailored (e.g. technology specific, site-specific, etc.) threat artifacts (e.g. reports, presentations, technical documents, etc.) to support the creation of technical objectives based on adversary capabilities, motivations, and tactics, techniques, and procedures to be used for assessment scoping and planning, briefing materials, or summary reports to senior management.
- Participate in assessment planning meetings (internal and external) to discuss threat artifacts and provide threat-related input to assessment strategy, focus, and objectives.
- Participate in assessment interviews and gather firsthand insights into vulnerabilities and threat scenarios to support additional insights during the end-of-day meetings, validation meetings, and out brief preparation.
- Collect assessment conclusions to support program-level reporting and add them to the Consolidated Assessment Review spreadsheet.
- Provide clear and concise explanations of the potential impact of identified assessment observations based on threat information in the reporting phase of assessments.
- Suggest improvements for integrating threat information into the assessment process in collaboration with the assessment leads and EA-60 leadership.
- Provide summary information pertaining to cybersecurity assessment results.

2.1.3 Federal Assessment Team Leaders

- Lead assessments of cybersecurity programs or topics when assigned.
- Ensure that subsequent cybersecurity assessment activities review the effectiveness of corrective actions using an approach that accounts for the significance and complexity of the issues.
- Provide direction and guidance to team members on the scope and approach to specific assessment activities.
- Work with EA-60 Director to develop and maintain a process guide for conducting cybersecurity assessments (this document).
- Support the EA-60 Director 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.
- Ensure assessment planning meetings are purposeful and provide required input to assessment activities.
- Leads the team in the creation of 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, with the support of contracting staff.
- Provide feedback on the proposed assessment team structure and make recommendations for the allocation of resources needed to accomplish the scope, ensuring that the assessment team is appropriately resourced to complete the assessment.
- Coordinate with site points of contact (POCs) for receipt of relevant documentation and artifacts prior to assessments.
- In coordination with the assessment team, ensure the schedule of events aligns with each assessment's scope and focus 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.
- In coordination with the assessment team, develop clear messaging for the results (e.g., context, why the assessment is important, content is appropriate for the audience) of the assessment and deliver them with the team during validation meetings, out briefs, and post-assessment briefings with EA or DOE senior management.
- Provide feedback on the overall assessment during the post-assessment meetings on what went well, what could be improved, and what EA-60 can change for next time.
- Proactively 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 that the report meets quality standards for clear messaging and accuracy and is appropriate for the intended audience.
- Immediately notify EA-60 Director of any impact related to assessment activities.
- Ensure the delivery of the report for FAR and QRB by the approved target dates.
- Provide summary information pertaining to cybersecurity assessment results to contribute to briefs and briefing materials for DOE managers and senior officials—including the Under Secretaries, Secretarial Officers, EA-1, and the EA-60 Director—and DOE policy organizations.
- Notify the EA-60 Director when assessment activities identify concerns that may have criminal or waste/fraud/abuse implications or any negative impacts from assessment activities.
- When assigned, lead the development of the annual National Security Systems and Office of Intelligence and Counterintelligence (IN) FISMA reports.

2.1.4 Programmatic and Technical Team Leaders

- Provide assessment results, development, report writing, and additional support to complete the annual National Security Systems and IN FISMA reports.
- Support the Federal assessment team leaders in coordinating and leading assessments of cybersecurity programs or topics.
- Provide input regarding assessment scope.
- Provide direction and guidance to team members on the approach to cybersecurity programmatic activities or technical performance testing that is aligned with assessment objectives.
- 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 assessment objectives.
- Develop the onsite assessment schedule and provide it to the Federal lead approximately four weeks prior to the assessment start date.
- 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 assessment team leader(s) 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 review per the approved timeline.
- Provide feedback on the overall assessment to the Federal assessment team leader.
- Develop a list of programmatic objectives (e.g., items to assess, determine, and ultimately find the answer to) unique to each assessment that supports the assessment team's ability to thoroughly assess each site's cyber program's effectiveness and ability to support the missions within the Department. Topical areas must also account for the following:
    - Latest DOE orders
    - Latest Program Office Program Plan, Execution Guidance, or equivalent
    - National Institute of Standards and Technology (NIST) Guidance
    - Committee on National Security Systems Instruction (CNSSI) Guidance
    - Latest DOE Office of the Inspector General (IG) FISMA metrics (as applicable to National Security Systems and Office of the Intelligence Community (IC) IG FISMA reports).
- Develop a list of technical objectives (e.g., items to assess, determine, and ultimately find the answer to) unique to each assessment that support the assessment team's ability to thoroughly assess each site's cyber program's effectiveness and ability to secure their mission by addressing the latest threats, vulnerabilities, and Departmental focus areas.
- Ensure all programmatic and technical objectives are complementary and align with what is most important to the site mission and to the Department.

- 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 and what may need to be done to remove files used by the technical team or to change authenticators derived during testing.
- Recommend initiatives to EA-60 Federal staff and contractor 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 assessment planning for improved assessment results.
- Provide rollup information pertaining to cybersecurity assessment results.
- Continuously research and expand Departmental knowledge to support well-informed assessments that provide an accurate and value-added status of cybersecurity programs across the Department.

2.1.5 Team Member(s): Cybersecurity Specialists (Programmatic Team) and Cybersecurity Performance Testing Specialists (Technical Team)

- Support the assessment and programmatic and/or technical team leaders and the Federal staff in planning, conducting, and reporting 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 assessment objectives.
- Provide input to update assessment objectives 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 staff and programmatic and/or technical team leaders.
- Assist in preparing the schedule of interviews to accomplish during assessment activities.
- Review key site cybersecurity documents obtained during the data call or through ongoing research prior to the assessment and provide input on missing or incomplete information to the assessment leads.
- Execute external technical performance tests and capture results in a standard format prior to the internal testing as applicable.
- Conduct thorough assessments in accordance with the assessment plan, the Federal assessment team leader, 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.

- Continuously research and expand Departmental knowledge to support well-informed assessments that provide an accurate and value-added status of cybersecurity programs across the Department.

2.1.6 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.

2.1.7 Technical Editor

- Edit assessment reports and annual FISMA reports. This includes independent editing, working closely with authors, participating in collaborative reviews, helping to resolve 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 EA 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 IC, and NIST.

EA-60 manages the areas of scheduling, budgeting, resource forecasting, and procurement as well as develops site and mission information that contain valuable data points, including FISMA metrics, Federal Risk and Authorization Management Program data, threat data (integrated Joint Cybersecurity Coordination Center [iJC3], Department of Homeland Security (DHS), open source, etc.), and plan of action and milestones 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, 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. 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-60 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-60 Director, 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 enable the safe and secure mission execution for the program or office being assessed. 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 1 provides a list of assessment types.

Table 1: 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. • Can be focused on technical effectiveness with limited programmatic review. • Can be conducted onsite or remotely • May involve touring facilities, attending meetings, participating in self-assessments, or shadowing other agencies in their audit activities. • Conducted to obtain current information about operations, activities, and initiatives at a site or within a program to support conclusions on the cybersecurity program's effectiveness.
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 Announced Assessments

Cybersecurity assessment processes, procedures, and tools are continually reviewed and refined to remain current with the threats and trends in cybersecurity. EA-60 applies each of these processes and tools according to the scope and scale of the assessment. Team members use a variety of assessment methods and performance tests to evaluate and identify strengths and weaknesses in a site's cybersecurity program. 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. When all observations (including technical observations where applicable) are gathered and analyzed for impact, the results culminate in a report that accurately reflects the status of the cybersecurity program assessed.

4.1.1 Programmatic Assessment Activities

Programmatic assessment activities are driven by relevant threat information, assessment focus, site mission, and overall Departmental priorities. Programmatic assessments are tailored to support the objective of identifying a cybersecurity program's ability to support the DOE mission safely and securely. This objective is supported by gathering data, analyzing program performance using documents requested and technical observations, and interviewing various site-, program-, or office-specific personnel.

4.1.2 External Performance Testing

External performance testing is primarily used to provide an overall assessment of a program's external network security posture. EA-60 conducts this assessment activity from EA-60's authorized Cybersecurity Testing Network. 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.
- Scanning for misconfigurations, open ports, or potentially vulnerable services to inform the site of potential risks.
- Validating that ownership of devices discovered during external performance testing is associated with the specific DOE site or program.
- Assessing the effectiveness of protection measures for internet-facing devices, application program interfaces, management interfaces, or other exposed services.

4.1.3 Internal Performance Testing

Internal performance testing evaluates the effectiveness of technical security measures and determines potential areas of vulnerability. Internal performance testing is 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. Testing can utilize site-provided systems, credentials, EA-60 systems, or a combination.

Using site-provided systems and credentials emulates an authorized user on the network. 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.

4.2 Unannounced Assessments

4.2.1 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. Internal performance testing may also be conducted in conjunction with an unannounced assessment activity, in which case such testing will be carefully coordinated with the trusted agents. 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 program that should be excluded from testing activities are known to the assessment team in advance. EA-60 communicates assessment milestones and their status to the white cell to track the overall process. Under no circumstances will testing occur without an approved assessment plan and coordination with DOE GC and the white cell.

4.2.2 Open-Source Information Gathering

The goal of OSIG 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. Technical teams 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. 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.

4.2.3 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. This is normally combined with OSIG and used during unannounced assessments. 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. Using these testing methods, the assessment team will evaluate the overall incident response process to determine the program's level of resiliency to such tactics.

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 or the white cell to ensure that the testing results help direct program improvements rather than consequences for any individual.

4.3 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.

4.4 Other Assessment Activities

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

4.4.1 Systematic Correlation and Analysis of Networks Program

The Systematic Correlation and Analysis of Networks (SCAN) program's 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 cybersecurity assessments, to identify 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, identify vulnerabilities, and to validate risk factors for the 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 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.

5 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.

Figure 1: Assessment Phases

5.1 Initiating

Figure 2: Initiating Phase

The goal of the initiating phase is to establish a strategic foundation for evaluating DOE's cybersecurity posture. This phase begins in early quarter two of the fiscal year to identify potential assessment

targets for the next one to three years, establishing a consistent rhythm of "always assessing" to ensure continuous oversight of critical programs. This proactive approach promotes a culture of continuous improvement and helps the Department stay ahead of evolving cybersecurity threats.

The initiating phase involves a thorough review of the Department's strategic priorities, leveraging several key resources:

- **DOE Primary Mission Essential Functions (PMEF) and Mission Essential Functions (MEF) matrices:** These matrices highlight the critical operations and systems necessary for achieving the Department's mission.
- **Threat Information:** Gathering and analyzing threat information, emerging cybersecurity requirements, relevant incidents, mission priorities, and historical knowledge to develop potential assessment targets.
- **Initial Threat Report**: Utilizing relevant iJC3 incident trends, reported incidents, known threat actor activity, attack surface metrics, and data calls. This product is used to recommend assessment focus areas as well as the most impactful threat scenarios of concern.
- **Stakeholder input:** EA-60 seeks input from various DOE program offices, site leadership, senior management, DOE IG, and GAO to understand the current priorities, concerns, and potential challenges associated with each target.

EA-60 uses the information from these resources to identify potential assessments that focus on areas of highest potential risk to the overall DOE mission.

EA-60 then begins shaping a flexible assessment timeline built on a formal annual schedule for the following calendar year; years 2 and 3 remain flexible and serve as the basis for planning the following year's priorities.

After the initial assessment target list is created, EA holds internal planning sessions to determine priorities and deconflict assessment schedules with all the EA offices. Once these meetings are complete and the initial draft of the schedule is created, EA-60 staff work with the site management and stakeholders such as the DOE IG to identify assessment overlaps and develop the final dates for the annual schedule. This deconfliction process is crucial to ensure that the schedule is feasible and adaptable.

At the beginning of the fiscal year, formal calendar year assessment announcement memos are created to send to each program office and the respective sites. The EA-60 Director, with support from the support services contractor (SSC), designates assessment teams and associated leads. The Federal staff and SSC will then initiate the creation of important milestone dates for reports. Projected QRB dates will also be set and used for coordination throughout the year.

Lastly, the schedule incorporates buffer periods and allows for the seamless integration of new assessments as required. This approach ensures that EA-60 can respond to critical cybersecurity concerns in a timely manner without compromising the overall effectiveness of the assessment program. If the schedule is changed, the EA-60 Director and/or Federal assessment team leader will inform the key internal stakeholders (e.g., other EA offices and the administrative assistant) and 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.

5.1.1 Initiating Inputs and Outputs

Table 2 lists the inputs and table 3 lists the outputs from the initiating phase of the assessment life cycle.

Table 2: Initiating Inputs

Input	Resources Needed	Responsible Party	Approximate Time Frame
Past assessment information; Current priorities; DOE PMEF/MEF; Threat Analysis	Threat reports; iJC3 incident information; SCAN output; PMEF/MEF Matrix; Stakeholder request information	Director with support from Federal and SSC staff	Available at the beginning of the Initiating phase and throughout the 1–3-year time frame

Table 3: Initiating Outputs

Output	Resources Needed	Responsible Party	Approximate Time Frame/Due Date
Assessment target list	All inputs above	Director with support from Federal and SSC staff	Quarter 2 of the Fiscal Year
Draft assessment schedule	Assessment target list	Director with support from Federal and SSC staff	Quarter 3 of the Fiscal Year
Final assessment schedule	Final list of planned assessment programs	Federal assessment leaders and SSC management	Completed each October
Calendar year assessment announcement memos	Finalized schedule	Director with support from Federal staff and SSC	Distributed at the beginning of the Fiscal Year
Report tracker development and QRB dates	Report tracker template	Administrative assistant; Technical editors	Developed in October

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's 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.

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

5.2.1 Planning Phase Activities

The assessment team initiates scoping and planning activities with senior Federal and contractor site management approximately 120 days prior to the assessment. This begins with the team working internally to develop the assessment strategy and to establish high-level objectives, assessment parameters, and site POCs. The timelines vary depending on the focus of the assessment and the overall priority. The assessment team establishes the scope of the assessment activities based on the reason for the assessment, the assessment objectives, and the needs of the Federal, programmatic, and technical teams to achieve those objectives. 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 the overall assessment strategy and what is most important to achieve the assessment objectives.

The assessment leaders review current information about the site, program, and other related threat information from the threat liaison 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 assessment team tailors all data calls based on the assessment strategy, objectives, and overall focus. The assessment team conducts a stakeholder engagement meeting to facilitate initial introductions between the site/program personnel and the EA team, provides a high-level overview of the EA assessment process if required, and requests additional information about the site that will be beneficial in the initial planning efforts. An initial data call may also be used to gather specific information related to the program. Additionally, the Federal assessment team leader may request a cyber program overview briefing, presented by the site, to provide additional insight into site mission and operations. The assessment team participates in these meetings by providing input, gathering information, and taking notes to use to inform the development of additional assessment questions, technical testing targets, and report writing.

Following the stakeholder engagement meeting, the assessment team, including the threat liaison, discusses the information and outcome of the meeting to validate, update, or create additional

objectives and a plan for follow-up meetings with the site/program. This is also the time when scope can be refined. An assessment planning meeting may be used to request additional cybersecurity program information, conduct exploratory interviews, discuss threat information, or determine other priorities or concerns the sites management may have. Additional meetings may be scheduled to assist in planning assessment logistics, clarifying data requests, or addressing assessment-related concerns. These meetings have the goal of preparing the team and the site to promote collaboration and successful accomplishment of the objectives of the assessment and to provide valuable results back to the site or program.

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

- Reviewing the threat report and discussing with threat liaison and assessment team members.
- Reviewing available program information (e.g., public information, internal DOE information, past reports, and 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 strategies that are unique to the site's mission, specific focus, and threat information to ensure the assessment team can effectively accomplish its objectives and successfully report on the status and effectiveness of the cybersecurity program.
- Identifying DOE HVAs, as applicable.
- Coordinating logistics with site personnel, including site access issues, conference room requirements, training requirements, shipping information, support needs, and deployment and use of remote assessment capabilities (when needed).
- Reviewing any data call information (initial or full) or other site-provided information.
- Adapting assessment strategies and objectives based on limited information, changes in priorities, or emergency assessment requests.
- Completing training and access requirements to ensure that the assessment can start immediately on the first day.
- Preparing, securing, and shipping the assessment equipment to the site.

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 requires an assessment plan that includes preliminary identification of the assessment scope; preliminary programmatic and technical team topics/targets; and assessment schedules, ROE, and trusted agent information. In those cases where there are joint assessment activities with other EA offices, a joint assessment plan is developed by all EA applicable team leaders. Every effort is made to

identify areas of emphasis in the assessment plan; however, the assessment is not limited to evaluating only the specific areas listed in the assessment plan.

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.

The Federal assessment team leader provides the assessment plan for approval by the EA-60 Director. The assessment plan is then sent to the site POCs and management in advance of the assessment for review and comment. 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 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 POCs of the condition in the unlikely event that performance testing adversely affects a system. Testing procedures targeting the affected system will resume only when 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 Assessment Data Call

The data call can be broken into two parts: an initial data call and full data call. Each part includes technical and programmatic document/information requests used to identify potential areas of interest or concern. The teams will use interviews or performance testing to follow up on these areas of interest and/or concern. If necessary, the assessment team will convene with the cognizant site/program office POCs, management, and subject matter experts to clarify any questions related to the data call or to request additional information. Sites are requested to send the data call information in a timely manner that supports sufficient review time prior to the assessment.

5.2.5 Logistics Information

The Federal assessment team leaders will work with 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:

- Inbrief on the first day of the assessment
- Technical testing
- Programmatic interviews
- Technical interviews
- Daily validation meetings
- End-of-day meetings for the EA assessment team
- Out brief preparation
- Out brief with the assessment team, site leadership, and site POCs

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

5.2.6 Assessment Schedule

The programmatic and the technical team leaders will develop an initial interview schedule and provide it to the Federal assessment team leader for site deconfliction. The Federal assessment team leader will also communicate conference room and virtual communications and collaboration requirements to the program's POC prior to the assessment activity to ensure adequate space, the necessary resources, and subject matter experts are available.

Some flexibility is built into assessment schedules to allow additional interviews if unexpected or unanticipated events occur during the assessment to fill data gaps, or to 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 assessment team will schedule daily informal validation meetings with site POCs and management starting on the second day of the assessment to provide feedback on the progress of data collection, areas requiring further review, and issues of potential concern, if any. Additionally, a management meeting with senior site management – for example, the Authorizing Official and the CISO – may be held as needed to briefly discuss the progress of the assessment results.

Due to the nature of unannounced assessments, a milestone schedule is developed to identify approximate time frames when the Federal assessment team leader will brief the program POCs, 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.

5.2.7 Planning Inputs and Outputs

Outputs from the initiating phase are considered inputs for the planning phase. Table 4 captures the additional inputs that occur within the planning phase itself. Table 5 lists the outputs from the planning phase of the assessment life cycle. Timelines are approximations and will depend on the type of assessment as well as overall assessment data requirements.

Table 4: Planning Inputs

Input	Resources Needed	Responsible Party	Approximate Time Frame
Assessment focus, initial assessment strategies, initial objectives	DOE research information, past assessment results, individual research output, threat information and reports, assessment strategy meeting (internal)	Assessment team	Prior to stakeholder engagement meeting
Site-provided mission and operational information	Site mission brief, site-provided initial data call, historical information, initial discussion output from initiating phase	Site POCs, Assessment team	After/during stakeholder engagement meeting

Table 5: Planning Outputs

Output	Resources Needed	Responsible Party	Approximate Time Frame
Tailored assessment threat report	EA-60 Resources, MEF/PMEF matrix	Threat Liaison	After assessment planning meeting
Tailored initial and/or full data call and request	Output from all meetings and input to date	Assessment team	After stakeholder engagement and/or planning meeting

Output	Resources Needed	Responsible Party	Approximate Time Frame
Assessment planning information	Assessment planning meeting, Site personnel, Meeting objectives, all inputs	Assessment team	After stakeholder engagement meeting
Solidified assessment objectives	Output from all meetings and input to date	Assessment team	After assessment planning meeting
Tailored data call artifacts	Tailored data call	Site POCs	Requested in a timely manner that supports sufficient review time prior to the assessment
Assessment schedule	Output from all meetings and input to date; Information garnered from data calls	Programmatic and technical leads; Federal assessment team leader(s)	Provided to sites at least 2 weeks prior to assessment (or as requested)
Assessment logistics request	Assessment schedule; Room requirements; Assessment planning meeting results	Federal assessment team leader(s)	Sent to assessment POCs after assessment planning meeting
Assessment plan	Assessment plan template; Output from all meetings and input to date	Federal assessment team leader(s) supported by SSC	Sent to EA-60 Director after draft completion
Assessment plan site review/signature	Reviewed assessment plan draft	Site POCs	Sent to EA-60 Director after draft completion
Logistics and travel plans	Concur; travel coordination spreadsheet	EA-60 Director; Federal assessment team leaders; Administrative assistant	4-6 weeks prior to the assessment
iJC3 and NNSA IARC notification (for external assessments)	iJC3/IARC notification email template, site POCs and contact information	Federal assessment team leader(s)	No later than 30 days 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	1-4 weeks prior to onsite assessment

Output	Resources Needed	Responsible Party	Approximate Time Frame
Visitor requests submitted and accepted by site POCs	Site visitor request forms; Training certificates	Federal assessment team leader(s); Administrative assistant; Site POC	3-4 weeks prior to the assessment
Follow-up meetings (as necessary)	Output from all meetings and input to date	Federal assessment team leader(s); Programmatic and technical team leaders	1-4 weeks prior to assessment
Assessment equipment is packaged and sent to site and tracking information shared	Standard technical image; Assessment hardware; Special requests from team; Inventory checklist; Shipping crates	Federal assessment team leader(s); Technical team leaders; Laboratory administrator(s)	At least 1-2 weeks prior to the assessment
Final inbrief slides sent to team and site POCs	Inbrief/briefing template	Federal assessment team leader(s)	1 week prior to the assessment

5.3 Conducting

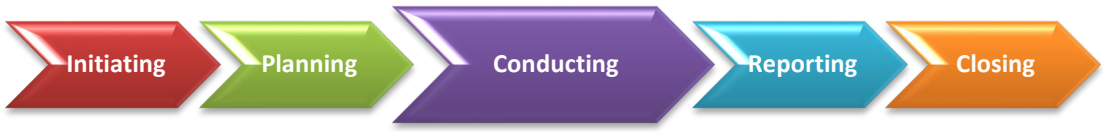

Figure 4: Conducting Phase

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 analyzes the in-place cybersecurity program to evaluate whether the current program is effectively supporting the overall risk management of the mission. During this stage, the team develops assessment conclusions based on analysis of data and validates information with site personnel.

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 mission needs. The assessment plan and ROE outline any specific or prohibited activities and are 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 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 evaluate the effectiveness of implemented controls and identify potential weaknesses. Technical team members develop and conduct performance testing strategies based on assessment planning knowledge and the characteristics of the program resources. Technical testing activity is also driven by information from the threat liaison. The threat liaison may provide specific use cases and tailored information gleaned from the research and development of the threat report and cross-referencing the planning information to come up with specific scenarios that should be tested to provide insight into the program's ability to identify and protect against threats.

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 also reviews the procedures and results from 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. Some assessments also include searches for wireless access points controlled by the program that may be vulnerable and allow access into the site's network. If vulnerabilities or weaknesses are identified that pose significant risk, 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 gather additional information to supplement any technical observations. Performance testing and interview results are also used as input for the programmatic review to determine specific weaknesses and to assist in identifying root causes of systemic problems. The combination of performance testing and review of essential program elements allows the assessment team to find potentially systemic concerns with process or other risk management implementation issues that could decrease the effectiveness of the program.

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 are 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-60 Director, who conveys 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. 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 maintain the integrity of the assessment while providing valuable site-specific information to maximize the allotted testing time. 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 artifacts supporting the performance of the program, and coordinates the results of these activities with members of the technical team to confirm if program performance is effective at managing risk and supporting the site's mission. The assessment team also specifically examines the sites' ability to protect against threats identified by the threat liaison and how the program uses the emerging threats 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 malicious activity to include malicious insider activity, as required by the Department, NIST, and CNSSI.

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 security measures. 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. This includes a review of the program's self-

assessment and issues management processes used to identify weaknesses and work to build enduring solutions to prevent them from recurring. 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 life cycle. Initial communication begins with the initiating and planning phases of the assessment. During onsite activity, the assessment team will provide routine feedback to the site POCs and management on the progress of the assessment, keeping site personnel informed of any potential concern associated with the review. This occurs during daily validation meetings, normally starting on the second day of the assessment. These meetings summarize the previous day's results provide an opportunity to validate those results and allow the assessment team leaders to ask any follow-up questions. The site POC and management has an opportunity and responsibility to communicate any concerns or adjustments to the factual accuracy of the information covered with the assessment team. 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 assessment team leaders present the pre-decisional results of the assessment to the key DOE field/site and contractor line managers. The pre-decisional closeout briefing focuses on a description of the strengths and weaknesses of the program and conclusions on the overall effectiveness developed by the assessment team. Specific findings may also be discussed due to the severity of such weaknesses.

Communication for unannounced assessments follows the established reporting timeline developed as part of the planning phase. EA-60 informs 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 team leader 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 leader 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. Selection of applications, tools, approaches, and implementation remains a line management responsibility.

5.3.4 Testing Conclusion Activities

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

- Notifying iJC3 and the NNSA IARC that testing activities are complete. (Federal leader)
- Conducting 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 and threat liaison including but not limited to specific issues to be called out in the report and their context. (Federal leader)
- 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 and the overall conclusion of the effectiveness of the program.
- Developing a written summary of the assessment observations and results and delivering it to the EA-60 Director and the assessment team. (Federal leader and threat liaison)
- Conducting post-assessment briefings with senior program office or EA officials related to assessment activities as requested. (Federal leader)

5.3.5 Conducting Inputs and Outputs

Outputs from the planning phase are considered inputs to the conducting phase. Table 6 lists the inputs and table 7 lists the outputs from the conducting phase of the assessment life cycle.

Table 6: Conducting Inputs

Input	Resources Needed	Responsible Party	Approximate Time Frame
Planning phase outputs	Threat report; Data call; Assessment objectives and strategy; Assessment schedule and logistics; Assessment plan	Federal assessment leader(s); Assessment team	First day of assessment
Assessment objectives and strategy	Assessment team consensus on questions to answer to determine effectiveness	Federal assessment leader(s); Assessment team	First day of assessment

Table 1: Conducting Outputs

Output	Resources Needed	Responsible Party	Approximate Time Frame

Commence external testing of the program-provided Internet Protocol ranges	Scanning systems setup; Data call	Technical assessment leader; Laboratory administrator(s); Technical assessment team	3-6 weeks prior to the assessment
Consolidated technical assessment data for delivery to site	Internal and external technical testing results; Technical team notes; Open-source information	Technical assessment leader	During assessment (tech data transfer)
Daily validation meeting content	Conducting inputs (see above); Programmatic and/or technical team analysis of results thus far; Site validation of results thus far	Federal assessment team leader(s); Programmatic and technical team leaders; Site POCs	Daily, during assessment activities
Pre-decisional out brief content	Conducting inputs (see above); Conclusions regarding program effectiveness (supported by program and technical team analysis and their observations)	Federal assessment team leader(s); Programmatic and technical team leaders; SSC management	End of the assessment
Notify iJC3 and the NNSA IARC of testing completion	iJC3/NNSA IARC closeout email template	Federal assessment team leader(s)	No later than one week post assessment
Assessment hotwash lessons learned	Assessment hotwash meeting; analysis of information; lessons learned	Federal assessment team leader(s); assessment team; SSC management	First week after return from the assessment
Summary of assessment conclusions	Out brief content; assessment objectives; assessment team input	Federal assessment team leader(s); assessment team; SSC management	4 days after return from the assessment
Consolidated assessment review update	Threat liaison assessment notes; Out brief content	Threat liaison	5 days post 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 officially communicate the effectiveness of the cybersecurity program based on the assessment observations. The Federal assessment team leader, with support for the SSC, 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, mitigating factors, and defense-in-depth capabilities to estimate their overall impact on performance. Weaknesses are considered in the context of controls that are relaxed during assessment activities, where the weaknesses are found, and the overall impact to the site's core mission functions. This analysis may lead to identification of deficiencies that cause specific weaknesses. The impact of those

deficiencies may result in them being categorized as findings. Factors that are considered during analysis of weaknesses include:

- Importance or significance of weakness.
- Compensating controls (defense-in-depth) 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.
- The level of access needed, the attack path used, and the controls that were relaxed that contributed to the weakness.
- Actual or potential effect on mission performance or accomplishment.
- Relevant DOE policy.

Threat liaisons also capture initial assessment observations during the assessment and prior to the out brief in the Consolidated Assessment Review spreadsheet. This is a document used to hold the results of compiled data from the assessments as they occur through the year. The spreadsheet serves as a running overview of the results found and the conclusions about the effectiveness of the programs. This allows EA-60 to quickly review areas of success/concern across the assessments performed and directly supports the identification of potential trends across the Department.

5.4.2 Report Preparation

The cybersecurity assessment report is prepared following the report tracker (i.e., schedule). All assessment team leaders are responsible for preparing the draft assessment report, ensuring it clearly addresses the conclusions about the effectiveness of the cyber program with the appropriate context and supporting detail. The designated lead writer has responsibility for the overall report with the support of programmatic and technical team members. The Federal lead and the threat liaison also play a role in the development of the report as a check to ensure accuracy of report details and the documentation of clear conclusions on the status of the cybersecurity program.

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-60 authorized derivative classifier during the onsite assessment to ensure that there are no spillage events *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 throughout the assessment phases to this point.
- The assessment team personnel review the draft report prior to the formal management review process ensuring all observations have the appropriate amount of context, outcome, and impact.

5.4.3 Collaborative Review Meetings

During the report development phase, the assessment team and SCC management review the report to ensure all observations contain the necessary context to support the conclusions from the analysis step of the assessment process. Additional reviews occur with EA-60 staff that were not present on the assessment and additional SCC management prior to the report being sent to the site for FAR. The technical editors finalize the document and remove the comments and edits from the reviews 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 use the matrix document to identify specific sections of the report where there are factually inaccurate statements and the necessary adjustments. Formal factual accuracy comments from the site are requested within five 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 reviews all factual accuracy comments and makes changes to the report, as appropriate. The FAR is not intended to eliminate conclusions or findings that the site POCs or managers view as unfavorable, nor is it intended to provide progress reports or changes in status that occur after the assessment is conducted. The assessments are designated as a "snapshot in time," and the assessment reports document the conditions in effect at that time. If it is determined that FAR comments identify an inaccuracy in the assessment information, EA may use follow-on interviews or documentation reviews to validate information provided and update the report as required.

The assessment team will work to adjudicate the comments, 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 Federal assessment team leader(s) for the QRB. The completed FAR comment matrix (i.e., with site comments and responses from EA) is provided to the administrative assistant for posting with the assessment folder as an assessment artifact.

5.4.5 Pre-QRB Collaborative Review

The newly updated report from the FAR is provided to the QRB members for their comments. Once each QRB member completes their review, the assessment team will work collaboratively on reviewing, understanding, and then addressing comments. Any comments that cannot be fully addressed should be discussed in a meeting with the assessment team and the QRB chair (i.e., EA-60 Director) prior to the formal QRB meeting. Once complete, the Federal assessment team leader(s) notifies the QRB members that comment adjudication is complete and requests a review of the updates.

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 edited, the Federal assessment team leaders will develop and send 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 it is then uploaded by the administrative assistant to the EA document repository for archival purposes.

5.4.8 Reporting Inputs and 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 with support from the assessment team and SSC management. Note, all specific deliverables are planned and scheduled using the report tracker. Table 8 lists the inputs and table 9 lists the outputs from the reporting phase of the assessment life cycle.

Table 8: Reporting Inputs

Input	Resources Needed	Responsible Party	Approximate Time Frame
Planning and Conducting phase outputs	Assessment objectives and strategy; Pre-decisional out brief content; Summary of assessment conclusions	Federal assessment team leader(s); Assessment team; SSC management	At the completion of the assessment
Report milestone due dates	Report tracker	Technical editor(s); SSC Management; Administrative assistant	Initial development at the beginning of the fiscal year; validated 2-3 weeks prior to assessment

Table 9: Reporting Outputs

Output	Resources Needed	Responsible Party	Approximate Time Frame
Draft assessment report for management review and resulting comments	Input from the assessment team members; Assessment conclusions and supporting information gathered during the assessment activities; Clear content that provides insight into the impact of results to the program; Initial tech edit	Federal assessment team leader(s); Lead writer; Assessment team; Technical editor(s); SSC management	25–30 days after the conclusion of the assessment
Draft report for FAR	Updated draft report from management review (PDF); FAR comment matrix	Federal assessment team leader(s); support from SSC Management, Assessment team, and Technical editor(s)	Report sent 1 day after receipt of draft report (approx. 35 days post assessment)
Site POCs FAR comments	FAR comment matrix	Site personnel	5 business days from receipt of FAR
Adjudicate FAR comments	Site-completed comment matrix	Federal assessment team leader(s);Lead writer; Assessment team; Technical editor(s); SSC management	2 days after receipt of FAR comments from site POCs and managers
Draft report for QRB review	Updated draft report based on FAR comments with final formatting	Federal assessment team leader(s); Lead writer; Assessment team; Technical editor(s); SSC management	6 days after receipt of FAR comments
QRB review comments	Draft formatted report	QRB members	5 days
Updated draft report from QRB comments	QRB comments; Assessment team edits based on comments	QRB members; EA-60 Director; Federal assessment team leader(s); Lead writer; Assessment team; Technical editor(s); SSC management	Approximately 52 days after the conclusion of the assessment

Output	Resources Needed	Responsible Party	Approximate Time Frame
Final assessment report generated based on finalized report from QRB	Updated draft report edited after QRB comment resolution	Federal assessment team leader(s); Lead writer; Assessment team; Technical editor(s); SSC management	Approximately 58 days after the conclusion of the assessment
Report package submittal (Draft report, summary, and TX memo)	Draft assessment report; Memo distribution list; TX memo template; Assessment summary template	Federal assessment team leader(s)	58 days after the conclusion of the assessment
EA-1 Approval of Report	Final assessment report; Assessment summary; TX Memo	Federal assessment team leader(s), administrative assistant	No later than 60 days after the conclusion of the assessment
Program Office Coordination	Final assessment report; Assessment report summary	EA Office of Resource Management; Administrative assistant	65-90 days after the conclusion of the assessment
Assessment Briefing to the Office of the Secretary	Final assessment report; Assessment report summary	EA-1, EA Office of Resource Management	70-90 days after the conclusion of the assessment
Notification to EA-60 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 valuable to DOE sites, Departmental managers, and other stakeholders. The EA-60 teams gather lessons learned after each assessment to document those things that went well and that should continue to be part of the process as well as how the team can be more adaptable. EA-60 team

members also conduct their own process improvement activities to better each assessment, especially within the planning stage.

The EA-60 Director also solicits feedback from DOE program, 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 ensure the factual accuracy of information in support of the conclusions 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*, Implementation of Department of Energy Oversight Policy*; and 205.1D, *Department of Energy Cybersecurity Program*. Each member of an assessment team has a role in documenting assessment activities for use in developing conclusions.

EA-60 does not retain large volumes of information to document assessment activities. All security requirements for the marking and handling of controlled unclassified information and classified documents are 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-60 Director to support development of the annual IG FISMA reports.

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

5.5.3 Records Retention

EA-60 uploads copies of the following documents to the EA document repository for each assessment activity.

- Signed assessment plan and Trusted Agent form
- Completed FAR comments matrix
- Final report, assessment report summary, and signed transmittal memo

5.5.4 Closing Outputs

Table 10 lists the outputs from the closing phase of the assessment life cycle.

Table 10: Closing Outputs

Output	Resources Needed	Responsible Party	Approximate Time Frame
Finalized copies of documents listed in section 5.5.3	EA document repository	Administrative assistant; Federal assessment team leader(s); Technical editors	Occurs automatically after review and approval action is closed, no more than 7 days after report distribution

Output	Resources Needed	Responsible Party	Approximate Time Frame
Purge assessment data	Access to shared repositories	Federal assessment team leader(s); Assessment team; Laboratory administrator(s)	15 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.

Consolidated Assessment Review – The Consolidated Assessment Review spreadsheet is a running record of assessment results that allows EA-60 to quickly review areas of success or concern across the assessments performed.

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 251.1E, Chg. 1, *Departmental Directives Program*. (DOE Directives, Guidance, and Delegations)

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.

Threat Report – A threat report is a comprehensive document that outlines potential security threats and vulnerabilities, and other pertinent information researched and shared with the assessment team in advance of the start the assessment. It is created and finalized through research and data gathering, open-source information, previous reports, and cybersecurity data. The report includes detailed analysis to tailor and focus a cybersecurity assessment. It serves as an additional resource to support the assessment leads and team when planning, conducting, and developing reports for assessments.

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 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 is used for deconfliction if unannounced assessment activities are discovered. The white cell also provides EA with any specific exclusion parameters to be used during unannounced testing activities.