U.S. DEPARTMENT OF
ENERGY

EA Enterprise Assessments

# Office of Cyber Assessment Operations

# Assessment Process Guide

**January 2023**

**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”. |

# Office of Cyber Assessment Operations
# Assessment Process Guide

## Approval Form

Approved by: CHRISTOPHER MCFEARIN Digitally signed by CHRISTOPHER MCFEARIN Date: 2023.01.24 11:31:35 -07'00'

Christopher E. McFearin
Director
Office of Cyber Assessments (EA-60)
Office of Enterprise Assessments

Acknowledged by: Timothy B. Schwab Digitally signed by Timothy B. Schwab Date: 2023.01.21 11:04:55 -05'00'

Timothy B. Schwab
Director
Office of Cyber Assessment Operations (EA-62)
Office of Enterprise Assessments

Table of Contents

# Acronyms

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

| | |
|---|---|
| KM | Knowledge Management |
| KMT | Knowledge Management Tool |
| NIST | National Institute of Standards and Technology |
| NNSA | National Nuclear Security Administration |
| NSS | National Security Systems |
| OCIO | Office of the Chief Information Officer |
| OFI | Opportunity for Improvement |
| POA&M | Plan of Action and Milestones |
| QRB | Quality Review Board |
| ROE | Rules of Engagement |
| SSC | Support Services Contractor |

# Executive Summary

The U.S. Department of Energy (DOE) Independent Oversight program is implemented by the Office of Enterprise Assessments (EA), according to the requirements established in DOE Order 227.1A, *Independent Oversight Program*, which identifies the Office of Cyber Assessments (EA-60) as the organization responsible for conducting cyber assessment activities for DOE sites and facilities. In addition, EA-60 conducts assessments of DOE and the National Nuclear Security Administration (NNSA) national security and intelligence systems to meet the annual independent evaluation requirements of the Federal Information Security Modernization Act of 2014.

DOE Order 205.1C, *Department of Energy Cyber Security Program*, formally delegates Secretarial Authority for cybersecurity to the Deputy Secretary. The Order assigns the EA Director the responsibility of providing independent oversight of the DOE cybersecurity program in accordance with EA's mission, functions, assigned responsibilities, and associated national requirements and DOE directives.

This Assessment Process Guide is part of an ongoing effort by EA-60 to maintain the quality, consistency, and contribution of the assessment program's activities and products. This guide outlines the methodology, procedures, tools, and techniques to accomplish these tasks.

To support this mission, EA-60 is organized into three offices:

- The Office of Cyber Assessments (EA-60), which is responsible for:
    - Management and oversight and Departmental coordination of cybersecurity assessments, reporting, and response.
- The Office of Cyber Assessment Strategy (EA-61), which is responsible for:
    - Evaluating, monitoring, and analyzing emerging cybersecurity threat information to enhance the overall effectiveness of cyber assessments.
    - Overseeing and managing Knowledge Management and Knowledge Development programs and capabilities to research and correlate cybersecurity information relevant to DOE and Office of Cyber Assessment Operations (EA-62) assessments.
    - Developing and implementing knowledge-sharing infrastructure to facilitate improved knowledge sharing and reporting.
    - Evaluating and providing subject matter expertise to develop and continuously improve the catalog of cybersecurity assessment capabilities.
    - Responding to specialized and ad hoc cybersecurity reporting requirements.
    - Analyzing cybersecurity trends and complex-wide issues to provide feedback on essential information assurance practices to DOE Headquarters and sites.
- The Office of Cyber Assessment Operations (EA-62), which is responsible for:
    - Conducting independent evaluations of the effectiveness of classified and unclassified cybersecurity policies and programs throughout DOE.
    - Maintaining a continuous program for assessing the security of DOE classified and unclassified networks through expert program and technical analysis, including detailed network penetration testing to detect vulnerabilities, configuration weaknesses, and other potential risks that could be exploited by sophisticated adversaries.

This Assessment Process Guide describes the continuous program for assessing cybersecurity by outlining the processes, techniques, and procedures used to evaluate DOE's cyber security programs. This includes both NNSA and contractor organizations' cybersecurity programs designed to protect the confidentially, integrity, and availability of DOE information systems. This also includes the protection of special nuclear material, classified information, Power Marketing, and sensitive unclassified information.

This Assessment Process Guide is part of an ongoing effort to maintain the quality, consistency, and contribution of the assessment program's activities and products. The assessment process has evolved through experience, and this process guide has been developed to be flexible and easily adaptable as it is applied during the various assessment activities conducted by EA-60. To ensure that this guide remains current and the assessment process continues to improve, all users of this guide are encouraged to provide comments and recommendations to the Director of EA-62 for consideration.

This Assessment Process Guide is a living document. It will be reviewed and, if applicable, updated at least annually. The approved version of the guide will be available on the Energy.gov website.

# Definitions

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

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

**Cognizant Manager** – The cognizant manager is the DOE field or Headquarters manager who is directly responsible for program management and direction including 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 implementation of an applicable requirement or performance standard. Deficiencies may serve as the basis for one or more findings. In accordance with DOE Order 227.1A Chg1, *Independent Oversight Program*, EA may use site- or program-specific equivalent nomenclature when assigning deficiencies and findings.

**Directives** – Directives are defined in DOE Order 251.1D Chg1, *Departmental Directives Program*.

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

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

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

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

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

**Performance Testing** – Performance testing is the conduct of activities to evaluate all or selected portions of systems, networks, or programs as they exist at the time of the test. Performance testing includes, but is not limited to, tabletop exercises, penetration testing, continuous automated scanning, and vulnerability scanning. Performance testing can be conducted as part of a scheduled assessment activity (i.e., announced), or with limited knowledge of the entity being tested (i.e., unannounced).

**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 leadership who are aware of the unannounced testing and will maintain the confidentiality of all assessment activities unless a situation warrants further communication to the site personnel. This white cell serves as the primary communication conduit for all activities and will be used for deconfliction in the event that unannounced assessment activities are discovered. The white cell will also provide EA with any specific exclusion parameters to be used during unannounced testing activities.

# 1 Introduction

The Department of Energy (DOE) Independent Oversight program is implemented by the Office of Enterprise Assessments (EA). The Office of Cyber Assessment Operations (EA-62), within the Office of Cyber Assessments (EA-60), is responsible for conducting independent cybersecurity assessment activities at DOE sites that possess high-value security interests, as mandated in DOE Orders 227.1A Chg1, *Independent Oversight Program*, and 226.1B, *Implementation of Department of Energy Oversight Policy*. EA-60 maintains its independence by having no direct responsibility for facility operations, protection program management, information systems management, or policy formulation.

## 1.1 Mission

EA-62's mission is to independently evaluate the effectiveness of classified and unclassified cybersecurity programs implemented throughout DOE. It facilitates consultative and assessments services to DOE and other government customers, leveraging established standards, leading practices, and applicable guidance specific to the relevant mission areas and operating environment. EA-62 accomplishes this by planning and conducting a variety of assessments that include programmatic and/or technical elements of the in-place cybersecurity operational, management, and technical controls. Programmatic assessments include examination of documentation, interviews, and discussions with key personnel and an overall assessment of the implemented cybersecurity controls. Technical assessments incorporate testing activities that simulate a broad range of threats to provide a complete and realistic evaluation of a site's cybersecurity posture at DOE and National Nuclear Security Administration (NNSA) field and operations offices and management and operating partner sites. The output from these assessments culminate in reports that provide recommendations and identify findings, deficiencies, opportunities for improvement, and best practices. Upon request, there can be follow-up reviews to ensure that site-specific corrective actions are effective.

This document provides additional insight into the assessment approach and processes associated with assessing classified and unclassified cybersecurity programs. Cybersecurity activities encompass the following:

- Periodic assessments of classified and unclassified cybersecurity programs at DOE sites.
- Cybersecurity assessments of information security programs.
- Periodic assessments of classified and unclassified cybersecurity intelligence programs at DOE sites.
- Remote testing of DOE internet-facing assets for vulnerabilities through scanning and penetration testing.
- Unannounced penetration testing of DOE sites and program office locations.
- Open source information gathering of DOE entities.
- Follow-up activities to ensure that identified issues are addressed in a timely and effective manner.
- Providing information for the Office of Assessment Strategy (EA-61) to support studies of cybersecurity issues across the DOE enterprise.
- Providing information for EA-61 to support ongoing analyses to identify cybersecurity trends and emerging issues within DOE.

- Development of recommendations and identification of opportunities for improving cybersecurity performance.
- Reviews of other governmental and commercial cybersecurity programs and frameworks to provide benchmarks for DOE performance.
- Assessments of the effectiveness of DOE policies governing classified and unclassified cybersecurity.
- Providing inputs for the annual evaluation of DOE's national security systems (NSS) and field intelligence elements (FIEs), as required by the Federal Information Security Modernization Act (FISMA) of 2014.
- Participation on the DOE Information Management Governance Board (IMGB).
- Participation in the DOE Insider Threat Working Group.
- Participation in the DOE Enterprise Architecture Governance Board.
- Participation in DOE Incident Response Leaders Forum
- Participation in DOE the Chief Information Security Officer (CISO) Roundtable

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

## 1.2 Scope

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

# 2 Governance

EA-60 is divided into two offices that work alongside one another to accomplish cybersecurity assessment for the departmental elements within DOE. EA-61 and EA-62 are governed by their respective directors and work with one another to share information and inform one another regarding assessments. The offices work together to inform future assessment strategies and add to the overall knowledge acquired during the assessments for trending and analysis. EA-61 in turn provides EA-62 with information from past reports, specific site-related information regarding mission and program office information, and also works to engage with the program offices and other senior DOE management to develop assessment priorities.

Figure 1 depicts the EA-60 organizations.

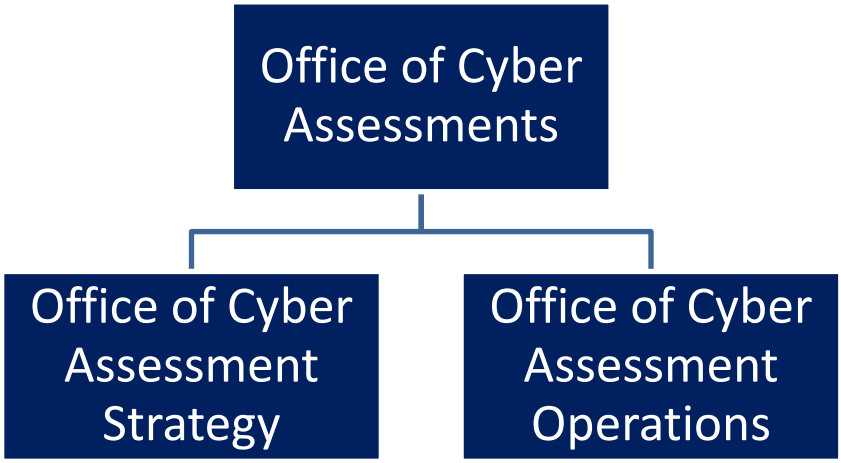


*Figure 1: Office of Cyber Assessments Organization*

## 2.1 Roles and Responsibilities

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

*Table 1: Roles and Responsibilities*

| Role | Responsibility |
|---|---|
| **EA-60 Director** | • Approve assessment reports prior to distribution to the Director, Office of Enterprise Assessments (EA-1).<br>• Distribute EA-1 approved reports to site management.<br>• Provide insights to and feedback of the overall assessment process.<br>• Serve as the Quality Review Board (QRB) chair for all EA-60 reports.<br>• Participate in DOE Cyber Council. |
| **EA-60 Deputy Director** | • Act on behalf of the director in managing all functions of the Office and is responsible for all Operations and Strategic Assessments functions within EA-60. |

| Role | Responsibility |
|---|---|
| | • Serve as technical monitor for the support services contract.<br>• Communicate status of activities for EA-60 to EA leadership and DOE Senior Leadership.<br>• Participate in the Intelligence Community (IC) Inspector General's (IG) quarterly meeting.<br>• Participate in QRB meetings. |
| **EA-61 Director** | • Work with the EA-62 Director to define and integrate assessment strategies that align with DOE mission priorities.<br>• Oversee and maintain the EA-60 Knowledge Management (KM) and Knowledge Development (KD) efforts to provide relevant information to inform the assessment process.<br>• Provide historical information pertinent to each assessment lead to use as part of the initial planning and scoping process.<br>• Provide trending information pertaining to cybersecurity assessments to the assessment leads.<br>• Analyze and provide relevant cybersecurity threat and trend information to inform the assessment process.<br>• Receive, process, and arbitrate new Federal requirements, DOE Directives, Policy, and other official guidance to make recommendations for inclusion into the assessment process.<br>• Participate in QRB meetings. |
| **EA-62 Director** | • Provide overall direction for and management for cybersecurity assessment operations within EA-60.<br>• Brief DOE managers and senior officials – including the Under Secretaries, Secretarial Officers, the EA Director, and the EA-60 Director – and DOE policy organizations on the results of assessment activities.<br>• Notify the EA-60 Director when assessment activities identify concerns that may have criminal or waste/fraud/abuse implications.<br>• Develop and maintain a process guide for conducting cybersecurity assessments (this document).<br>• Ensure that subsequent cybersecurity assessment activities review the effectiveness of corrective actions using a tailored approach based on significance and complexity.<br>• Work with cognizant DOE line managers and policy organizations to resolve disagreements on assessment schedules, results, findings, or OFIs.<br>• Participate in QRB meetings.<br>• Participate on the DOE IMGB.<br>• Participate in the IC IG quarterly meeting.<br>• Act as system owner for all assessment-related information technology (IT) resources.<br>• Provide coordination, coaching, and oversight of Federal assessment team leaders in the conduct of assessments. |

| Role | Responsibility |
|---|---|
| | • Designate a senior Federal employee to serve in the role of Operations Manager, in addition to their other assigned duties (will assume both roles if Operations Manager is not designated)<br>• Provide assessment results and other required information to the EA-61 to assist in trending and analysis.<br>• Participate the DOE Office of the Chief Information Officer (OCIO) High Value Asset (HVA) working group and Department of Homeland Security (DHS) Assessments of the DOE HVA program (or designee)<br>• Work with the EA-61 Director to integrate assessment strategies that align with DOE mission priorities.<br>• Support the EA-60 KM and KD efforts to capture relevant information about the assessment process and provide the data to EA-61. |
| **Operations Manager** | • Participate in DOE data calls and strategic initiatives<br>• Develop and maintain an office work plan to Federal assessment team leader positions for upcoming assessments.<br>• Conduct a final quality assurance review of assessment activities and reports.<br>• Chair pre-QRB meetings<br>• Participate in QRB meetings<br>• Serve as a Federal assessment team leader<br>• Serve as CyberScope subject matter expert.<br>• Participate on the DOE IMGB.<br>• Obtain feedback from stakeholders on the assessment process.<br>• Document lessons learned and incorporate into the overall assessment process.<br>• Participate and contribute to the DOE Insider Threat Working Group.<br>• Develop plans of action and milestones (POA&Ms) for the development and implementation of new tools, tactics, and procedures to enhance cybersecurity assessments.<br>• Maintain tracking information for delivery of key milestones related to assessment activities to include but not limited to planning activities, report development, and report delivery.<br>• Monitor overall assessment process and brief the EA-62 Director on status of key milestones. |
| **EA-62 Federal Assessment Team Leaders** | • Provide direction and guidance to the assessment team members consistent with the EA-62 Director's instructions.<br>• Recommend assessment schedules.<br>• Serve as Federal assessment team leader for assessments when designated by the EA-62 Director.<br>• Support the EA-62 Director in interfacing with DOE Headquarters and field personnel to coordinate activities and address concerns.<br>• Chair both the management review board meetings for assessments where they are the lead.<br>• Participate in QRB meetings. |

| Role | Responsibility |
|---|---|
| | • Lead assessments of cybersecurity programs or topics.<br>• Lead assessment scoping meetings and provide input to assessment activities.<br>• Provide direction and guidance to team members on the approach to specific assessment activities.<br>• Draft scoping slides, cybersecurity assessment plans, data calls, and other assessment briefings.<br>• Manage system access for site personnel to online repository for data calls.<br>• Provide feedback on proposed assessment team structure and make recommendations for allocation of resources needed to accomplish the scope while ensuring that we are maximizing resources and limiting team size.<br>• Coordinate with sites for receipt of site documents prior to assessments.<br>• Coordinate with team and site on logistics for assessment, including requests for appropriate resources needed for the assessment.<br>• Establish the schedule of events during cybersecurity assessments and deliver to the site.<br>• Ensure that team members perform their assigned duties before, during, and after the assessment.<br>• Address site concerns associated with assessment activities.<br>• Provide feedback to site personnel daily to validate assessment information and clearly communicate areas of concern.<br>• Oversee preparation of and present assessment reports.<br>• Review and provide feedback to the assessment report, that ensures accuracy of results and appropriate messaging for the intended audience.<br>• Brief site management and cybersecurity personnel on assessment results.<br>• Immediately notify EA-62 and EA-60 Directors of any impact related to assessment activities.<br>• Brief EA and DOE senior management on assessment results.<br>• Ensure the delivery of the report for QRB per the approved targets.<br>• Ensure the posting of the final report and associated information to EA Share and the delivery of information to EA-61.<br>• Provide feedback on the overall assessment to the Operations Manager and EA-62 Director.<br>• Develop and distribute the initial direction for the assessment report in the designated format. |
| **Programmatic and Technical Team Leaders** | • Provide support in preparing the annual NSS and Office of Intelligence and Counterintelligence (IN) FISMA reports.<br>• Provide support in preparing the EA Annual Report.<br>• Support the Federal assessment team leaders in leading assessments of cybersecurity programs or topics.<br>• Provide input on recommended assessment scope. |

| Role | Responsibility |
|---|---|
| | • Provide direction and guidance to team members on the approach to cybersecurity programmatic activities or technical performance testing.<br>• Provide input to the Federal assessment team leaders on document requests and other necessary logistics to support the assessment team.<br>• Provide feedback on proposed cybersecurity assessment team structure and make recommendations for allocation of resources needed to accomplish the scope.<br>• Develop the schedule of interviews and make specific assignments.<br>• Ensure that team members perform their assigned duties.<br>• Address site concerns associated with programmatic or technical performance testing activities.<br>• Provide feedback to site personnel daily to validate assessment information and clearly communicate areas of concern.<br>• Participate in briefing site management and cybersecurity personnel on assessment results, as required.<br>• Prepare the programmatic and technical sections of the cybersecurity assessment report.<br>• Work with the team leader to resolve site comments on the assessment report.<br>• Participate in collaborative review meetings throughout the report development cycle.<br>• Participate in pre-QRB meetings.<br>• Participate in QRB meetings.<br>• Deliver report for QRB per the approved targets.<br>• Provide feedback on the overall assessment to the Operations Manager and EA-62 Director.<br>• Develop and maintain a list of programmatic topical areas required to thoroughly assess the cybersecurity programs within the Department that accounts for the latest Department Orders and Directives as well as National Institute of Standards and Technology (NIST) and Committee on National Security Systems Instruction (CNSSI) Guidance.<br>• Develop and maintain a list of technical topical areas required to thoroughly assess the cybersecurity programs within the Department that accounts for the latest threat, vulnerability, and Departmental focus areas.<br>• Ensure consistent assessment of all relevant topical areas on each assessment.<br>• Ensure that technical information gathered during the assessment is delivered in the agreed-upon format and captures the necessary details to inform the site of any weaknesses or vulnerabilities discovered.<br>• Refine existing processes and develop the required initiatives to improve technical assessment capabilities. |

| Role | Responsibility |
|---|---|
| | • Propose enhancements to existing infrastructure and capabilities in order to perform advanced research into adversaries' practices and tactics, to increase understanding of advanced threats, and to incorporate knowledge gained into standard assessment procedures for improved assessment results. |
| **Team Members**<br><br>**Cybersecurity Specialists (Programmatic Team)**<br><br>**and**<br><br>**Cybersecurity Penetration Testing Specialists (Technical Team)** | • Support the assessment and programmatic and/or technical team leaders in conducting assessments of cybersecurity programs or topics.<br>• Provide input to the assessment and programmatic and/or technical team leaders on assessment scope and potential approaches for accomplishing cybersecurity assessments.<br>• Provide input to update assessment topical areas to include the latest Departmental Orders/Directives and the latest NIST and CNSSI guidance.<br>• Conduct assessment activities following direction and guidance of the Federal assessment team leaders, and programmatic and/or technical team leaders.<br>• Assist in preparing the schedule of interviews to accomplish during assessment activities.<br>• Review key site cybersecurity documents prior to the assessment and provide input on missing or incomplete information to the assessment leads.<br>• Execute external technical penetration tests and capture results prior in a standard format prior to the internal testing as applicable<br>• Conduct thorough assessments in accordance with the assessment plan, the Federal assessment team leaders, and the programmatic and/or technical team leaders.<br>• Validate assessment data and conclusions with site personnel daily to ensure factual accuracy.<br>• Participate in briefing site management and cybersecurity personnel on assessment results, if requested.<br>• Consolidate technical information obtained during external and internal portions of the assessment.<br>• Provide written input for draft assessment reports, as directed by the Federal assessment team leader and programmatic and/or technical team leaders.<br>• Work with the programmatic or technical leader to resolve site comments on the assessment report.<br>• Serve as information system security officers (ISSOs) for EA IT resources, as assigned.<br>• Follow established assessment protocols and standards for each assessment.<br>• Acknowledge annually, through signature, the elements of this Assessment Process Guide. |

| Role | Responsibility |
|---|---|
| **Administrative Assistant** | • Maintain the assessment artifacts (report, assessment plan, and review history) for all cybersecurity assessments in the approved EA repository.<br>• Maintain the assessment report folders in the approved EA repository and update EA-60 report milestones for EA leadership.<br>• Collect and provide archive of information and data related to program management activities from the cybersecurity assessments to EA-61.<br>• Assist with management and control of physical records system, records organization and evaluation, and inactive records system.<br>• Develop and maintain internal and external report correspondence.<br>• Serve as travel coordinator.<br>• Schedule collaborative reviews, pre-QRB, and QRB meetings.<br>• Obtain conference call-in numbers and WebEx or other screen-sharing meetings.<br>• Maintain assessment calendars for EA distribution and external stakeholders.<br>• Coordinate transmission of report drafts throughout the Reporting phase of the assessment process including processing of review and approval workflows.<br>• Post final version of report, transmittal memo, and assessment summary for EA-60 Director concurrence and EA-1 approval.<br>• Coordinate the creation of the final report, including the appropriate transmittal memo for distribution and providing it to the EA-60 Director.<br>• Closing out assessment folder and finalizing assessment artifacts as part of the Closing phase of the assessment.<br>• Posting EA-60 unclassified assessment report title to Energy.gov. |
| **Cybersecurity Laboratory Administrator** | • Manage the Cyber Security Test Network (CSTN) and Cyber Assessments Mobile Platform (CAMP) to ensure their reliability in supporting assessments in accordance with the approved security plans.<br>• Notify the CSTN ISSO of any planned changes prior to their implementation.<br>• Secure the CSTN and CAMP by developing network access, monitoring, control, and evaluation processes and maintaining documentation.<br>• Prepare users by designing and conducting training programs, and providing references and support.<br>• Upgrade the CSTN and CAMP by conferring with vendors and developing, testing, evaluating, and installing upgrades and enhancements. |
| **Technical Editor** | • Edit assessment reports and annual FISMA reports. This includes independent editing, working closely with authors, participating in collaborative reviews, helping to adjudicate feedback from the QRB |

| Role | Responsibility |
|---|---|
| | and site factual accuracy review (FAR), and proofreading reports before they are submitted for approval routing.<br>• Manage the report editorial process.<br>• Edit point papers as requested by Federal assessment team leaders and EA-62 Director.<br>• Review and edit ad hoc white papers, data calls, and reports.<br>• Edit additional products as requested by the EA-60 team (e.g., the Assessment Process Guide, Change Control Board draft, network reauthorization packages, etc.).<br>• Other duties: Additional writing, editing, or presentation development projects as assigned. |

# 3 Collaboration and Interfacing with External Organizations

There is significant value in collaborating and interfacing with other DOE Headquarters program offices, field/site offices, and DOE and NNSA site 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 within each office internally and interfaces with organizations external to DOE, such as the White House, Congress, the Intelligence Community, and NIST.

Within EA-60, the offices collaborate in the areas of scheduling, budgeting, resource forecasting, and procurement. EA-61 develops Site Portfolios that contain valuable data points including FISMA metrics, Federal Risk and Authorization Management Program (FedRAMP) data, threat data (Joint Cybersecurity Coordination Center [iJC3], DHS, open source, etc.), and POA&M data. Site Profiles are provided to EA-62 in support of assessment planning. EA-61 may also pass along requests from external entities such as Insider Threat Working Group and the Privacy Office that can be scoped and appropriately tasked.

EA-62 has partnered with the DOE OCIO and the DHS in the assessment of the Department's 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, IG, and Environmental Management. 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. Lastly, individuals within the office participate on the DOE Cyber Council and DOE IMGB. EA has also established partnerships with the DOE IG, the DOE GC, and the OCIO, who receive copies of all assessments.

## 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 similar to 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 is recommended in writing (emails are acceptable) by the applicable DOE Headquarters or field/site office and is selected and approved for participation by the EA-62 Director. Recommendations must come from the senior Federal manager and must include the specific objective and overall intention of the augmentee's participation.
    - Augmentees 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 topic team to which they are assigned.
- DOE and other government agency observers are recommended in writing (emails are acceptable) by the applicable Federal agency manager and are approved by the EA-62 Director. Recommendations must come from the senior Federal manager and must include the specific objective and overall intention of the observer's participation.
- Observers are assigned to one or more topic teams during an assessment activity but do not conduct data collection activities.

# 4 Assessment Types

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

*Table 2: Assessment Types*

| Assessment Type | Description |
|---|---|
| **Announced and Unannounced Assessments** | Assess the effectiveness of one or more aspects of a site's classified and/or unclassified cybersecurity program, as defined in the assessment scope.<br>A focused assessment can include technical testing and/or less extensive programmatic review.<br>All assessments are conducted to obtain current information about operations, activities, and initiatives at a site or within a program, and may involve touring facilities, attending meetings, participating in self-assessments, or shadowing other Agencies in their audit activities. |

| Assessment Type | Description |
|---|---|
| **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 testing a site's cybersecurity posture using realistic threat scenarios. |

## 4.1 Assessment Activities

Cybersecurity assessment processes are continually reviewed, refined, and applied according to scope and scale of the assessment. Processes, procedures, and tools used are also adjusted, modified, and updated to remain current with the threats that new cybersecurity technology introduces.

Cybersecurity assessment activities use a systematic approach that includes examination of the management, operations, and technical controls and technical performance testing, in order to conduct thorough and objective assessments. Team members use a variety of assessment methods and performance tests to evaluate and identify strengths and weaknesses in a site's cybersecurity program. Performance testing provides a good snapshot of the effectiveness of technical implementation but does not provide insight into the sustainability and direction of the program. Technical weaknesses that are identified through performance testing are generally symptoms of larger, more pervasive problems associated with management of the site's cybersecurity program. Therefore, a significant emphasis is placed on complementing technical performance testing with a programmatic review to assess the effectiveness of key underlying management processes associated with cybersecurity programs. This approach results in identification of systemic issues and provides a basis for evaluating the direction and sustainability of the associated cybersecurity programs.

### 4.1.1 Programmatic Assessments Activities

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

### 4.1.2 Technical Assessments Activities

#### *4.1.2.1 Announced External Penetration Testing*

Announced penetration testing is typically conducted in conjunction with an announced cybersecurity assessment of a program. Announced activities are primarily used to provide an overall assessment of a site's network security posture. These assessment activities are conducted from EA-62's CSTN. External penetration testing may consist of:

- Scanning network systems exposed to the internet for vulnerabilities and attempting exploits to evaluate the potential impact of weaknesses.
- Scanning site wireless networks to identify unauthorized or misconfigured wireless access that could provide an alternative route into the network.

- Leveraging DOE OCIO external testing capabilities and leveraging their results or assisting sites with understanding the impact.

#### *4.1.2.2 Unannounced Penetration Testing*

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

#### *4.1.2.3 Internal Penetration Testing*

The key goal of internal penetration testing is to evaluate the strength of internal boundaries that provide isolation between differing need-to-know environments and to determine potential areas of vulnerability with the in-place cybersecurity technical controls. Internal penetration testing is typically conducted onsite for announced assessments and may be applied to either classified or unclassified resources. Internal testing may also occur remotely depending on the nature and scope of the assessment. Testing can utilize site-provided systems, EA-62 assets, or a combination of both. The technical team is provided a central location from which most scanning and penetration testing activities are conducted. However, some testing must be conducted from various points within the site's network. Internal penetration testing may also be conducted in conjunction with an unannounced assessment activity, in which case such testing will be carefully coordinated with the trusted agent(s).

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

#### *4.1.2.4 Continuous Network Scanning*

The Continuous Network Scanning (CNS) program is a function designed to systematically review the internet-facing presence of all DOE organizations and catalog the web servers and other external network connections accessible by the general public. CNS is focused on identifying DOE network borders and implementing technology and not on the content of websites. EA documents the CNS capabilities and the overall program description in the *Continuous Network Scanning Program Whitepaper.*

The primary goals 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).
- Obtain information gathered by external publicly accessible third parties, such as ARIN, Google, and SHODAN, as it pertains to DOE cybersecurity assets.

- Catalog internet-facing application information, such as web server type and version.
- Provide a single comprehensive location for current information describing the DOE network perimeter for use in conducting independent oversight activities.
- Provide initial reconnaissance information for external penetration tests as part of a specific cybersecurity assessment.
- Provide a framework for additional special-purpose scans of the DOE external internet presence.

Information from CNS may be used on any type of assessment, but also may be shared with stakeholders at the sites, DOE and NNSA OCIO, as well as other internal stakeholders with the appropriate need to know.

#### *4.1.2.5 Open Source Information Gathering*

The goal of open source information gathering is to identify potential targets that an adversary may use for cybersecurity attacks against information systems and phishing or other social engineering attacks against a site or the larger DOE enterprise. This information allows the technical team to perform its own assessments, including human vulnerability assessments, and to evaluate the cybersecurity program's operational security measures to prevent information from being exposed to the public.

As part of the external assessment process, the technical team will review social media and other internet sources to look for people, information (e.g., blueprints, maps, photos) regarding the physical location, and potential leakage of controlled unclassified information to the public. If the technical team identifies a potential weakness, they will immediately notify the site so that the site can take immediate action. The open source information is bundled into the information provided to the site at the end of every assessment. Overall, 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 to the sites for operational security awareness.

#### *4.1.2.6 Phishing/Human Vulnerability Testing*

The goal of the human vulnerability assessment is to test the susceptibility of personnel identified during the open source information gathering to phishing or other social engineering methods commonly used by DOE's adversaries. Before such activities begin, these methods will be discussed and agreed upon via the assessment plan, where both EA and the site agree to the overall rules of engagement.

These tests are not intended to identify poor performance of specific individuals, but rather to focus on improving the cybersecurity programs. The assessment leads will work with the local sites to ensure that the testing results are not seen as punitive against any individual.

This testing will also use various means to identify potential areas of weakness in the technical controls that should prevent successful phishing or other attacks, as well as test the overall performance of the site's detection methods. During these simulated attacks, the assessment team will evaluate the overall incident response process to determine the site's level of resiliency to such tactics.

### 4.1.3 Special Assessments

EA-62 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 about testing a site'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 as an office will work with the involved stakeholders to leverage its combined knowledge to support the assessment efforts.

### 4.1.4 Other Assessments Activities

As requested by DOE leadership, internal DOE organizations, or external partner organizations, EA-62 will conduct assessments or technical testing activities to evaluate the effectiveness of cognizant organizations' cybersecurity programs and activities. Prior to commencement of all assessment activities, a meeting with the stakeholders is held to determine the scope and duration. During this time, assessment milestones are developed and their status communicated to the white cell to track the overall process. After the scope is determined, the Federal assessment team leader assigned to the assessment/testing activity will follow the assessment phases, where applicable.

# 5 Assessment Phases


*Figure 2: Assessment Phases*

All cybersecurity assessments include five major phases: initiating, planning, conducting, reporting, and closing. Although these phases are identified as separate entities, they are not a linear process and may overlap with one another. Subsequent sections of this document describe the activities and expectations associated with each of the assessment phases. Templates for the associated assessment artifacts described in the "output" tables of Sections 5.1 – 5.5 are available in the template repository on the EA-60 SharePoint site.

## 5.1 Initiating

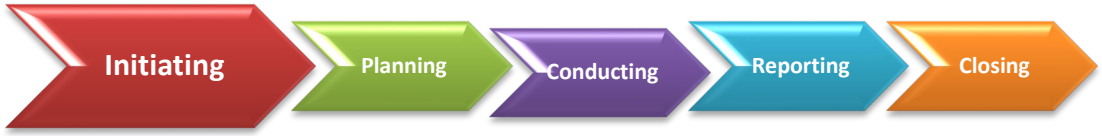


*Figure 3: Initiating Phase*

During the third quarter of each fiscal year, the Directors of EA-60, 61, and 62, in conjunction with EA leadership, conduct internal planning sessions to determine priorities for sites and programs to be considered for assessments during the following calendar year. This process involves engaging stakeholders from across the DOE enterprise, analyzing past assessment information from EA-61,

evaluating requests for assessments from the program offices, and evaluating priorities presented from DOE senior leadership. Once these meetings are complete and the initial draft of the schedule is created, the EA-62 Director works with the site line management to factor potential schedule conflicts and develop the final dates. The EA-62 Director prepares and sends formal calendar year assessment schedule memo for the EA-60 Director to send to each Program Office and the respective sites. This process necessitates the creation of the annual cybersecurity assessment integrated master schedule. This schedule identifies planning activities, key milestones, and resources required to conduct each assessment activity.

If the schedule is changed throughout the year, the EA-62 Director will inform the key stakeholders of the affected program office and site, along with the DOE IG.

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

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

### 5.1.1 Initiating Inputs and Outputs

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

*Table 3: Initiating Inputs*

| Input | Resources Needed | Responsible Party | Timeframe |
|---|---|---|---|
| Past assessment information; Current priorities | Schedule prioritization from Knowledge Management Tool (KMT); Stakeholder request information | EA-61 Director with support from the EA-61 teams | Available at the beginning of the Initiating phase. |
| Points of Contact for Program Office; Prospective sites | KM Information | Logistics points of contact | Available at the beginning of the Initiating phase. |

*Table 4: Initiating Outputs*

| Output | Resources Needed | Responsible Party | Timeframe/Due Date |
|---|---|---|---|
| Formal calendar year assessment memos | DOE stakeholder consensus | EA-62 Director | Delivered each October and documents the activities for the next calendar year. |
| Assessment Schedule | Final list of planned assessment sites | EA-62 Director | Completed each October. Consists of scheduled activities for the next calendar year. |
| Commence CNS reconnaissance | DOE site's internet protocol (IP) address range; CNS hardware/software | Technical team | Performed continuously, with a focus on scheduled assessments for the next calendar year. |
| Site Profile development | KMT; Previous assessment reports | EA-61 Director | Initial list of scheduled locations established in October every year with delivery of each Site Profile at least 90 days prior to each assessment. |
| Report Tracker development | Report tracker template | Administrative assistant; Logistics points of contact | Developed in October of each year for scheduled assessment activities. |

## 5.2 Planning


*Figure 4: 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. For example, an external network security assessment that is conducted remotely from the public internet requires less planning than a full assessment.

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

### 5.2.1 Planning Phase Activities

The EA-62 Director or the Federal assessment team leader initiates scoping and planning activities with senior Federal and contractor site management at least 6 to 8 weeks (or more) prior to the assessment to solicit input for the assessment scope and to establish high-level agendas, assessment parameters, and site and assessment team points of contact. This phase will establish the scope of the assessment activities, while also planning their execution and the follow-on phases. As part of this process, the

assessment leaders (Federal, programmatic, technical, and SSC management) review the assessment teams identified during the initiating phase and adjust the plan based on past experience at the site, the site's size, and the overall scope of the assessment. For example, technically focused assessments would not require a full programmatic team.

The Federal assessment lead conducts a pre-scoping meeting to facilitate initial introductions between the site and EA team, provide a high-level overview of the EA assessment process, request the initial data call, and request additional information about the site that will be a benefit in the initial scoping meeting. A key element to this process is the EA-61 created Site Profiles that outline key information pertaining to site (e.g., overall mission, number and name of FISMA systems, past report information, etc.). This information provides background to assist the assessment team in developing their initial scope and framing their questions as well as ensuring that the team can make the most efficient use of time by knowing the background of the site in question. Additionally, the Federal assessment team leader will request that the site prepare a mission brief, presented by site personnel during the scoping meeting, to provide an overview of the operations and mission at the site.

Following the pre-scoping meeting, the assessment team conducts a scoping visit (in person or virtually). This meeting allows all assessment team members to meet key site personnel, request additional cybersecurity program documentation, conduct exploratory interviews, and determine how key areas can be assessed effectively. Additional meetings (in person or virtual) may be scheduled to assist in defining the scope and establishing assessment process.

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

- Establishing assessment parameters based on Site Profile information and input from Program Office or site management.
- Reviewing available program information (e.g., past reports, corrective action plans).
- Identifying cybersecurity and FISMA systems that will be assessed.
- Identifying HVAs, as applicable.
- Coordinating logistics with site personnel, including site access issues, conference room requirements, training requirements, shipping information, and support needs.
- Coordinating logistics with site personnel for the deployment and use of remote assessment capabilities (when needed).
- Preparing an assessment plan, including preliminary identification of systems/networks to be inspected, reviewed, or tested; developing preliminary programmatic assessment/review topics and interview schedules, rules of engagement (ROE), and trusted agent forms.
- Reviewing any initial data call information requested during initial discussions with the Program Office or site.
- Developing and transmitting a request to the site for documentation (data call).
- Conducting one or more scoping call meetings.
- Planning travel and lodging arrangements for team members.
- Reviewing information provided by the site in response to the team's data call request.
- Identifying potential problem areas.
- Conducting external network performance testing.
- Shipping the assessment computers to the assessment site.
- Finalizing travel logistics (if necessary).

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

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

### 5.2.2 Assessment Plan

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

Unannounced assessments will begin with meetings with the white cell representatives, where an initial scope and rules of engagement is 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, EA-62, and site approvals, DOE GC and the EA-1 Director will review the plan to ensure they have awareness and visibility into the process.

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

### 5.2.3 Rules of Engagement

The ROE contained in each assessment plan outlines the respective roles and responsibilities of assessment team, site Federal and contractor cybersecurity managers, and trusted agents for the performance testing. The ROE explains the general approach and defines specific parameters and controls that will be followed during testing. The ROE includes the following general controls:

- Protect all information (classified and unclassified) from unauthorized access in accordance with DOE Orders.
- Suspend testing at the request of the site if there are legitimate safety, security, or operational concerns.
- Maintain frequent communications with the site with respect to the status of testing activities, including the coordination for any additional testing of systems at other locations where IT resources are deployed.

- Provide detailed information and work with cybersecurity and/or IT personnel to return information systems to the original configuration upon completion of testing so that no systems remain in a compromised state.
- Immediately terminate testing and notify the primary and secondary points of contact of the condition in the unlikely event that performance testing adversely affects a system. Testing procedures targeting the affected system will resume only once the system state is stable and testing procedures have been modified to prevent further disruptions.
- Inform the integrated iJC3 and/or NNSA Information Assurance Response Center (IARC) of performance testing dates to ensure that testing activities are not mistaken for real attacks.
- Identify any data developed by use of scanning activities or any data developed as a result of successful exploitation(s) and provide it to site management.
- Obtain approval from the site Authorizing Official or Authorizing Official Designated Representative prior to any data leaving the site.
  Follow the site's standard operating procedures and not reconfiguring network defenses to block, monitor, or filter testing activities.
- Identify any data developed during scanning activities or data developed because of successful exploitation(s) and provide it to the site trusted agent(s) and ISSM.
- During the assessment, provide the assessment team, through the trusted agent, with alerts or other indicators of activity that would trigger your 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 site is 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. In addition, the site must identify any system that is connected to the site network but is not under the direct control and responsibility of the site. Based on this information, the Federal assessment team leader may exclude some cybersecurity systems from performance testing activities.

### 5.2.4 Programmatic Data Call

The programmatic data call is broken into two parts: the initial data call and full data call. The Federal assessment team leader requests the initial data call during the pre-scoping meeting. The data call will be coordinated with the site prior to the formal sign-off of the Assessment Plan to ensure all parties have adequate time to gather the assessment artifacts prior to the assessment date. The initial data call documents requested are due 7 days after the pre-scoping meeting, and the full data call documents are due at least 30 days prior to the assessment unless otherwise stated. If necessary, the programmatic team will convene with the cognizant site/program office leadership and subject matter experts to discuss the data call and logistics for the assessment at least 2 weeks prior to the assessment. Data call document requests may include:

- Applicable local policies used for the management of the cybersecurity program, such as local processes and procedures. Local policies may include site work instructions or procedures addressing account management, configuration management, auditing and continuous monitoring requirements, incident response, or other programs elements.
- Relevant memorandums of understanding and/or Interconnection Security Agreements, including any with the DOE.

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

### 5.2.5 Technical Data Call

In addition to the programmatic data call, EA-62 will also request technical information to be delivered on the same schedule. If necessary, the technical team will convene with the cognizant site/program office leadership and subject matter experts to discuss the data call and logistics for the assessment at least 2 weeks prior to the assessment. Technical information may include:

- Technical points of contact for network, information systems, and telephone exchange systems; the point of contact data should include office telephone numbers, email addresses, and off-hour contact information.
- All IP ranges (including internal, external, IPV4, and IPV6) associated with the mission, IT, and cybersecurity programs at the site, including a list of IP addresses to be excluded from testing and a detailed justification for the exclusion.
    - EA will review the exclusions along with justification and coordinate with the site to determine alternative means of testing (such as special testing hours, manual scanning instead of automated scanning, etc.).
- Inventory of network endpoints, including approximate number of Windows and Linux/Mac/UNIX desktops and servers.
- A list of systems within the site address range that are requested to be excluded for safety, security, or other reasons; this list should include the IP addresses and the reasons for exclusion.
- A network topology map containing perimeter devices and IP addresses of those devices (including the main border router and other routers that have separate internet connections), firewalls, gateways, and major subnet routers.
- Router access control lists, firewall rules, and intrusion detection/prevention rules.
- Latest vulnerability scan results from the site's scanning system.
- Information related to any wireless networks in use, including service set identifier and media access control addresses of all authorized access points.

### 5.2.6 Logistics Information

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

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

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

### 5.2.7 Assessment Schedule

The programmatic and technical leaders are responsible for planning and conducting the programmatic and technical aspects of the assessment, such as interviews, document reviews, external performance testing (including penetration testing), internal performance testing, and tabletop reviews. SSC management, in coordination with the assessment team leader and the programmatic and technical

leaders, assign team members to support the programmatic and technical aspects of the assessment, as needed.

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

The assessment schedule is designed to efficiently use limited time during the assessment to ensure a thorough assessment is conducted. The schedule must address the critical data collection activities needed to satisfy the scope defined in the assessment plan. Some flexibility is built into assessment schedules to allow additional interviews if unexpected or unanticipated events occur during the assessment, or to fill data gaps or clarify information. The development of the assessment schedule requires extensive coordination with the site to set up interviews, walkthroughs, tabletop reviews, and validation meetings.

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

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

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

### 5.2.8 Planning Inputs and Outputs

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

*Table 5: Planning Inputs*

| Input | Resources Needed | Responsible Party | Timeframe |
|---|---|---|---|
| Scoping and planning call or in-person meeting | Federal assessment team leaders, technical and programmatic leaders, and site/program office stakeholders | Federal assessment team leader | 6 weeks prior to the assessment |

| Input | Resources Needed | Responsible Party | Timeframe |
|---|---|---|---|
| Coordinate receipt of Site Mission Brief | N/A | Federal assessment team leaders | 6 weeks prior to the assessment |
| Completed data call request to EA-62 | Feedback from the site; Data call delivery method | Federal assessment team leaders | 4 weeks prior to the assessment |
| Completed assessment plan; Posted to DocShare | Feedback from the site | Federal assessment team leaders; Administrative assistant | 3 weeks prior to the assessment |

*Table 6: Planning Outputs*

| Output | Resources Needed | Responsible Party | Timeframe/Due Date to/from Site |
|---|---|---|---|
| Scoping slides and meeting agenda | Scoping slides template | Federal assessment team leaders | 8 weeks prior to the assessment |
| Setting up and creating agenda for scoping and planning call or in-person meeting | Federal assessment team leaders, technical and programmatic leaders, and site/program office stakeholders | Federal assessment team leaders; Programmatic and technical team leaders | 6 weeks prior to the assessment |
| Completed assessment interview schedule sent to team and site | Information garnered from data calls; Inputs form the scoping and planning call or in-person meeting | Federal assessment team leaders; Programmatic and technical team leaders | 6 weeks prior to the assessment |
| Conference room logistics request sent to site | Assessment schedule; Room requirements; Scoping meeting results | Federal assessment team leaders | 6 weeks prior to the assessment |
| Results from CNS scanning activities for specific site | DOE site's IP address range; CNS hardware/software | Technical Team | 6 weeks prior to the assessment |
| Assessment plan (to include site points-of-contact and rules of engagement) | Assessment plan template; document request template | Federal assessment team leaders | 4 – 6 weeks prior to the assessment |
| Data call request provided to site | Data call template | Federal assessment team leaders | 4 – 6 weeks prior to assessment |

| Output | Resources Needed | Responsible Party | Timeframe/Due Date to/from Site |
|---|---|---|---|
| Logistics and travel plans | Concur; travel coordination spreadsheet | EA-62 Director; Federal assessment team leaders; Administrative assistant | 4 weeks prior to the assessment |
| Site specific CNS results | CNS reconnaissance results | Technical team leader | 4 weeks prior to the assessment |
| iJC3 and NNSA IARC notification (for external assessments) | iJC3/IARC notification email template | Federal assessment team leaders | 4 weeks prior to the assessment |
| Completed site required training and application for physical/logical access | Site-supplied forms and training materials/ instructions | Federal assessment team leaders; Programmatic and technical team leaders; Programmatic team; Technical team | 3 weeks prior to the assessment |
| Visitor requests submitted and accepted by site | Site visitor request forms; training certificates | Federal assessment team leaders; Administrative assistant; Site point of contact | 3 weeks prior to the assessment |
| Trusted agent/technical team planning meeting | Information garnered from data calls | Federal assessment team leaders; Programmatic and technical team leaders | 2 weeks prior to assessment |
| Assessment equipment setup and shipping preparation | Standard technical image; Assessment hardware; Special requests from team | Technical team leaders; Laboratory Administrator | At least 2 weeks prior to the assessment |
| Assessment equipment sent to site | Assessment equipment; Inventory checklist; Shipping crates | Federal assessment team leader; Administrative assistant; Technical team leaders; Laboratory Administrator | 1 week prior to the assessment |
| Final in-brief slides sent to team and site | In-brief/ briefing template | Federal assessment team leaders | 1 week prior to the assessment |

| Output | Resources Needed | Responsible Party | Timeframe/Due Date to/from Site |
|---|---|---|---|
| Site logistics email to team | Logistics email template | Federal assessment team leaders; Administrative assistant | 2 – 4 days prior to the assessment |

## 5.3 Conducting


*Figure 5: Conducting Phase*

The goal during the Conducting phase is to collect sufficient information regarding the performance, direction, and sustainability of classified and unclassified cybersecurity programs. During the Conducting phase of the assessment, the assessment team conducts performance testing and performs a programmatic review to evaluate essential underlying management processes. This phase includes varied activities, such as external assessments, interviews, walkthroughs, tabletop reviews, and data analysis that are customized to accurately assess the site's ability to protect its classified and unclassified information. During this stage, the team develops assessment conclusions based on analysis of data and validates information with site personnel.

To gain insight into a site's cybersecurity programs and to understand interdependencies with other site activities, the assessment uses a "bottom-up" approach to program assessment. As a first step, unclassified cybersecurity assessments will begin with extensive external network performance testing. This performance testing, including attempts to penetrate the site's network, is conducted remotely over the internet using DOE authorized information systems. The technical team will also perform penetration testing internally to mimic the tactics of an insider. The technical team may also conduct tabletop reviews of information systems excluded from performance testing, firewall rules, and intrusion detection systems to fully assess the implementation of the security controls. As noted in the Planning section, the assessment team leaders will review any site request and site justification for exclusion of certain critical safety or operational systems from testing to determine the proper testing activities.

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

### 5.3.1 Technical Approach

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

The technical team may also use site-provided computer systems and user credentials to emulate a trusted insider and/or a computer system compromised by an external attacker on the site's network. During this process, the technical team can determine whether locally available tools or other techniques might expose weaknesses with current configurations. In conjunction with this testing, the technical team will also review the testing procedures and results with the site's incident responders to determine whether there are opportunities to improve the site'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 is comprised of 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, Supervisory Control and Data Acquisitions, critical safety systems, or Internet of Things devices to determine whether weaknesses exist that could pose a risk to the site's mission or to personnel. Cybersecurity assessments also include searches for wireless access points controlled by the site that may be vulnerable and allow access into the site's network. The exploitation of vulnerabilities is performed to determine the impact to the enterprise, the detection and response capabilities of the site, and is conducted in coordination with the trusted agent. If egregious vulnerabilities are identified, testing is halted, and the site is informed of the vulnerability and given the opportunity to provide remediation or mitigation.

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

Unannounced assessments will follow a similar structure to announced assessments and will use many of the same techniques and leverage the same expertise to attempt to compromise the site information systems. The primary difference between these and announced activities is that the assessment team

will be working 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 may be conducted post performance testing with site personnel to understand more about the response actions taken or understand why a particular test was successful or not successful. All of these activities will be scheduled and coordinated as part of the ongoing assessment process.

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

#### *5.3.1.1 Trusted Agent*

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

Collaboration between the assessment team and local representatives must be open and professional to provide maximum value. The assessment team and the trusted agent(s) should approach cybersecurity assessments in a collaborative manner to ensure that these activities result in better protection levels for DOE IT resources. This collaborative approach is especially important during penetration testing, where trusted agents are used to maximize realism while maintaining the confidentiality of the scenario or test content and the timing of scheduled, limited-notice, and no-notice tests. All trusted agents sign a Trusted Agent Roles and Responsibilities Acknowledgement form (incorporated in the operations document) prior to being briefed on sensitive test information. Finally, the assessment team shares performance test materials with trusted agents in person or, when necessary, by encrypted email. These materials should not be forwarded to anyone who does not have a need to know.

### 5.3.2 Programmatic Approach

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

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

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

### 5.3.3 Communication and Feedback

The objective throughout each assessment activity is to ensure that a thorough and accurate assessment of a site's cybersecurity program is conducted and that site personnel gain maximum benefit from the experience. To accomplish this, the assessment team, site managers, and site cybersecurity staff must all communicate effectively. This communication begins prior to the assessment activities and continues throughout the assessment lifecycle. Initial communication begins with the scoping process and the development of the assessment plan and ROE, and continues during the assessment activities, beginning with an in-brief to site personnel on the scope, interview schedule, and report preparation process. Site management will then provide an initial mission briefing with an overview of the site's mission, cybersecurity program, resources, and any changes that have occurred since the planning meetings or the last assessment. Following these high-level briefings, the programmatic and technical teams meet with their respective site points of contact to begin the assessment activities.

During both performance testing and programmatic reviews, the assessment team will provide routine feedback to the site on the progress of the assessment, keeping site personnel informed of any potential concern associated with the review. This interchange occurs during morning validation meetings, normally starting on the second day of the assessment. These meetings summarize the previous day's activities, any observations related to the assessment, and allows the assessment team leaders to ask any follow-up or validation questions. The site has an opportunity and responsibility to provide feedback or concerns about factual accuracy. The site should provide additional data and identify site personnel who can help identify corrections for any factual accuracy misunderstanding. The activities listed in section 5.3.4 are integrated into the assessment process to ensure that the assessment team and site managers and staff have an opportunity to effectively communicate. If necessary, the Federal assessment team leaders will hold supplementary meetings with the site or field office Federal staff or management regarding key observations as applicable.

At the conclusion of an assessment, the Federal assessment team leaders or the EA-62 Director presents the pre-decisional results of the assessment to the key DOE field/site and contractor line managers,

highlighting program strengths, any identified weaknesses, and areas for improvement related to the site's classified and unclassified cybersecurity programs. The pre-decisional closeout briefing may be limited to a high-level summary of scope and pre-decisional results because more detailed validation meetings with site personnel were held during the assessment period, while more senior management personnel usually attend this closeout briefing.

Communication for unannounced assessments will follow the established reporting timeline developed as part of the planning phase. EA-62 will inform the white cell and other stakeholders as negotiated during the planning process on the current 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 will work with the white cell for approval if necessary. If at any time during the assessments the team determines that the site is at risk of attack based on an identified vulnerability, the Federal assessment team leaders will immediately notify the site of the issue so that the site 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, the assessment team is open to conducting a dialogue on technical issues. As an assessment organization, EA-62 does not direct a site to take any specific action, use any specific cybersecurity tools, or adopt any specific technical solutions. Rather, the assessment team will engage in technical dialogue to provide feedback on the advantages and disadvantages of specific applications, approaches, and implementation. Selection of applications, approaches, and implementation remains a line management responsibility.

### 5.3.4 Testing Conclusion Activities

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

- Notifying iJC3 and the NNSA IARC that testing activities are complete.
- Conducting a retrospective meeting with members of the assessment team to gather lessons learned.
- Providing an assessment point paper to the programmatic and technical assessment team leaders that serves as a summary and overall direction for the report; the point paper will also be delivered to the EA-60 and EA-62 Directors for awareness.
- Conducting post assessment briefings with senior Program Office or EA officials related to assessment activities as requested.

### 5.3.5 Conducting Outputs

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

*Table 7: Conducting Outputs*

| Output | Resources Needed | Responsible Party | Timeframe/Due Date |
|---|---|---|---|
| Commence external testing of the site-provided IP ranges | Scanning hardware and software;<br>Site data call | Technical assessment leader;<br>Technical assessment team | 4 weeks prior to the assessment |

| | | | |
|---|---|---|---|
| Consolidate external assessment data for delivery to site | Scanning results; Open source information | Technical assessment leader | 1 week prior to assessment |
| Consolidate assessment data for delivery to site | Internal and external scanning results | Technical assessment leader | End of the assessment |
| Daily validation meetings | Daily input from the programmatic and/or technical team | Federal assessment team leaders; Programmatic and technical team leaders | Daily during assessment activities |
| Pre-decisional closeout briefing | Consolidated daily input from the programmatic and/or technical team | Federal assessment team leaders; Programmatic and technical team leaders | End of the assessment |
| Notify iJC3 and the NNSA IARC of testing completion | iJC3/NNSA IARC closeout email template | Federal assessment team leaders | First day of return from the assessment |
| Assessment retrospective email | Assessment retrospective email template | Federal assessment team leaders | First business day after return from the assessment |
| Develop point paper; send to team and EA-62 Director | Point paper format | Federal assessment team leaders | 2 days after return from the assessment to the lead writers; finalized within 5 days from the assessment. |
| Results of assessment retrospective | Assessment team responses | All assessment team members, including team leaders | 21 days after return from the assessment |
| Analytical data gathered during the assessment activities | Daily input from the programmatic and/or technical team | Federal assessment team leaders; Programmatic and technical team leaders | End of the assessment |

## 5.4 Reporting


*Figure 6: Reporting Phase*

At the conclusion of each assessment, a validated report is published. 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 assessments may include deficiencies, which in accordance with DOE Order 227.1A Chg1, *Independent Oversight Program*, represent inadequacies in the implementation of an applicable requirement or performance standard. EA 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 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 reports, they may also address other conditions observed during the assessment process. OFIs are provided only as recommendations for line management consideration. Finally, EA 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 in order to prepare an assessment report and inform site management of results. Reports are sent 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.

Weaknesses are analyzed both individually and collectively; they are balanced against strengths and mitigating factors to estimate their overall impact on performance. This analysis may lead to identification of deficiencies that cause specific weaknesses. Factors that are considered during analysis of weaknesses include:

- The importance or significance of the weakness.
- Compensating controls implemented within the information system.
- Whether the weakness is isolated or systemic.

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

### 5.4.2 Report Preparation

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

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

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

- The team prepares the initial draft report consistent with the data collected and information that has been validated during the initiating, planning, and conducting phases of the assessment.
- The respective team leader and assessment team personnel review the draft report prior to the formal editorial process.
- The Federal assessment team leaders provide the report to the site for FAR.
- The QRB reviews the draft report to ensure that it is readable, logical, and contains adequate, balanced information to support the conclusions.

### 5.4.3 Collaborative Review Meetings

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

### 5.4.4 Draft Report Distribution for Factual Accuracy Review

The technical editors provide a new copy of the report to the Federal assessment team leaders who creates and provides a comments resolution matrix to the site, along with the initial draft report. The site uses the matrix document to identify specific sections of the report where the site has a factual accuracy comment. Formal factual accuracy comments from the site are requested within 5 working days after receipt of the draft report. Reports associated with the assessments of FIEs are also provided

to the DOE Headquarters IN Cyber Directorate for factual accuracy comments during this same five-working-day period.

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

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

### 5.4.5 Pre-QRB Collaborative Review

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

### 5.4.6 Quality Review Board

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

### 5.4.7 Finalizing the Report

Once all comments have been adjudicated and the report is formatted, the Federal assessment team leaders will develop a transmittal memo and assessment summary document to provide to the administrative assistant to route for approval by the EA-60 Director, and then for EA-1 concurrence. A final report is emailed by the administrative assistant to the EA-60 Director for electronic distribution and then uploaded to DocShare for archival purposes.

Notification of the final report distribution is also provided to EA-61 for inclusion in future planning, analysis, or trending of activities for EA-60.

### 5.4.8 Reporting Outputs

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

*Table 8: Reporting Outputs*

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

| Output | Resources Needed | Responsible Party | Timeframe/Due Date |
|---|---|---|---|
| Federal assessment team leaders submits to administrative assistant for distribution to QRB | Final formatted draft report | Federal assessment team leaders; Administrative assistant | 1 day after receipt of final formatted draft report |
| QRB review | Final formatted report | QRB members | 5 days |
| Conduct QRB and generate updated draft report | Final formatted draft report with adjudicated QRB comments | QRB members;<br>EA-60 Director;<br>EA-62 Director;<br>Federal assessment team leaders;<br>Lead writer;<br>Assessment team members assigned writing duties;<br>Technical editors | Approximately 56 days after the conclusion of the assessment; scheduled and coordinated after initial assessment schedule is developed |
| Final assessment report generated based on finalized report from QRB | Updated draft report from QRB review | EA-62 Director;<br>Federal assessment team leaders;<br>Lead writer;<br>Assessment team members assigned writing duties;<br>Technical editors | Approximately 58 days after the conclusion of the assessment |
| Transmittal memo and Assessment Summary | Final assessment report;<br>Memo distribution list | Federal assessment team leaders | 58 days after the conclusion of the assessment |
| Notification to EA-61 of final report distribution | Review and approval ticket | Administrative assistant | Automatic notification sent once review and approval ticket is closed |

## 5.5 Closing


*Figure 7: Closing Phase*

The Closing phase includes all the activities necessary for the assessment team leaders 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-62 supports the concept of continuous improvement in order to make cybersecurity assessments more effective and of value to DOE sites, departmental managers, and other stakeholders. The Operations Manager and/or EA-62 Director is responsible for soliciting feedback from each team member and making process improvement recommendations.

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

### 5.5.2 Documentation of Assessment Activities

The assessment team members collect a large volume of data and information through performance testing, document reviews, and interviews. The assessment processes are designed to assure the factual accuracy of information presented in assessment reports, and information is retained to provide supporting evidence. This documentation of results is necessary to fulfill EA-62's mission of conducting the annual evaluation of DOE classified information technology systems and providing input to the annual FISMA reports, as required by and DOE Orders 227.1A Chg1, 226.1B, and 205.1C. Each member of an assessment team has a role in documenting assessment activities for use in developing conclusions. The EA-62 Director, with support from the Operations Manager, is responsible for ensuring that key assessment information is captured and retained in formal documentation.

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

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

### 5.5.3 Records Retention

EA-62 maintains copies of the following documents on DocShare for each assessment activity:

- Signed site assessment plan
- Report comments matrix
- Final report, with transmittal memo

### 5.5.4 Closing Outputs

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

*Table 9: Closing Outputs*

| Output | Resources Needed | Responsible Party | Timeframe/Due Date |
|---|---|---|---|
| Finalize copies of documents listed in Section 5.5.3 | DocShare | Administrative assistant; Federal assessment team leaders | Occurs automatically after review and approval action is closed no more than 7 days after report distribution |
| Purge assessment data | Access to shared repositories | Federal assessment team leaders; Programmatic and technical team leaders | 15 days after report distribution |
| Lessons learned documented and posted to EA Share | Assessment retrospective; site feedback; EA-60 Director feedback | EA-62 Director and/or Operations Manager | 30 days after report distribution |
| KMT update | Final report; Assessment team feedback | EA-61 | 30 days after report distribution |