



U.S. DEPARTMENT OF
ENERGY



Office of Cyber Assessments (EA-21)
Assessment Process Guide



Version 7.0

July 29, 2016

Office of Cyber Assessments
Office of Enterprise Assessments
U.S. Department of Energy

This page is intentionally left blank.

| Document Version Control | | | |
|---------------------------------|---------------------------------|-----------------------|--|
| Version Number | Change Editor | Date of Change | Description of Changes Made |
| 1.0 | Derek Adams | March 29, 2013 | Original Document |
| 1.1 | Derek Adams | April 9, 2013 | Appraisal Process List |
| 2.0 | Derek Adams | May 13, 2014 | Post Re-Org / Name Change |
| 2.1 | Derek Adams | July 2, 2014 | Modify Roles & Responsibilities, Update Assessment Plan Sample |
| 3.0 | Derek Adams | Nov. 13, 2014 | Organization Name Change |
| 3.1 | Tarra D. Anthony | August 14, 2015 | Update Appraisal Guide |
| 3.2 | Tarra D. Anthony | September 2, 2015 | Update Appraisal Guide |
| 3.3 | Tarra D. Anthony | September 9, 2015 | Update Appraisal Guide to include changes from the EA APP |
| 3.4 | Tarra D. Anthony | October 1, 2015 | Update Appraisal Guide to include changes from the EA APP |
| 3.5 | Tarra D. Anthony | November 2, 2015 | Updates per EA-21 Director Changed appropriate "appraisal" references to "assessment" |
| 4.0 | Tarra D. Anthony/Jannett Moran | November 19, 2015 | Finalized per technical edit to the entire document. |
| 5.0 | Tarra D. Anthony | February 3, 2016 | Updated to include new DOE 227.1A definitions. |
| 5.1 | Tarra D. Anthony | February 18, 2016 | Updated to include title change and new processes. |
| 6.0 | Tarra D. Anthony/Chris McFearin | May 20, 2016 | Updated to include new processes, appendices, and EA-20 Director's comments throughout the document. |
| 6.1 | Tarra D. Anthony | July 6, 2016 | Update section 7.2.3 |
| 7.0 | Tarra D. Anthony/Chris McFearin | July 29, 2016 | Updates to sections 7.0 subsections to update output tables, 7.4.6 to include timeline for posting unclassified report titles to EA Website. and Appendix A, |

Table of Contents

| | |
|---|-----|
| Acronyms..... | v |
| Preface..... | vi |
| Definitions | vii |
| 1.0 Introduction | 1 |
| 1.1 Mission | 1 |
| 1.2 Scope | 2 |
| 2.0 Applicable Laws, Orders, Policies, and Standards..... | 3 |
| 3.0 Governance..... | 5 |
| 3.1 Roles and Responsibilities..... | 6 |
| 4.0 Collaboration and Interfacing with External Organizations | 9 |
| 4.1 Site Representatives..... | 9 |
| 5.0 EA-21 Assessment Teams | 10 |
| 5.1 Technical Team | 10 |
| 5.2 Programmatic Team..... | 10 |
| 6.0 Assessment Types | 11 |
| 6.1 Assessment Testing Activities | 11 |
| 6.1.1 Programmatic Assessments..... | 12 |
| 6.1.2 Announced Penetration Testing | 12 |
| 6.1.3 Unannounced Penetration Testing..... | 12 |
| 6.1.4 Internal Penetration Testing | 13 |
| 7.0 EA-21 Assessment Phases..... | 14 |
| 7.1 Initiating..... | 14 |
| 7.1.1 Initiating Outputs | 14 |
| 7.2 Planning | 15 |
| 7.2.1 Planning Phase Activities | 16 |
| 7.2.2 Rules of Engagement..... | 17 |
| 7.2.3 Technical Data Call..... | 18 |
| 7.2.4 Programmatic Review Data Call | 18 |
| 7.2.5 Assessment Plan..... | 19 |
| 7.2.6 Onsite Assessment Schedule | 20 |
| 7.2.7 Planning Outputs..... | 20 |
| 7.3 Conducting | 21 |

| | | |
|--|--|----|
| 7.3.1 | Technical Review | 22 |
| 7.3.2 | Programmatic Review | 23 |
| 7.3.3 | Communication and Feedback | 23 |
| 7.3.4 | Conducting Outputs | 25 |
| 7.4 | Reporting | 26 |
| 7.4.1 | Analysis of Results | 26 |
| 7.4.2 | Findings, Deficiencies, Recommendations, and Opportunities for Improvement | 27 |
| 7.4.3 | Report Preparation | 27 |
| 7.4.4 | Pre Quality Review Board Meeting | 28 |
| 7.4.5 | Quality Review Board | 29 |
| 7.4.6 | Report Distribution | 29 |
| 7.4.7 | Reporting Outputs | 29 |
| 7.5 | Closing | 30 |
| 7.5.1 | Process Improvements | 30 |
| 7.5.2 | Documentation of Assessment Activities | 31 |
| 7.5.3 | Records Retention | 31 |
| 7.5.4 | Closing Outputs | 31 |
| Appendix A: Assessment Program Outputs | | 32 |

List of Tables

| | |
|---|----|
| Table 1: Laws, Regulations, Policies, and Standards | 3 |
| Table 2: Roles and Responsibilities | 6 |
| Table 3: Assessment Types | 11 |
| Table 4: Initiating Outputs | 15 |
| Table 5: Planning Outputs | 20 |
| Table 6: Conducting Outputs | 25 |
| Table 7: Reporting Outputs | 29 |
| Table 8: Closing Outputs | 32 |
| Table 9: EA-21 Assessment Program Outputs | 32 |

List of Figures

| | |
|--|----|
| Figure 1: EA-21 Organizational Chart | 5 |
| Figure 2: EA-21 Assessment Phases | 14 |

| | |
|----------------------------------|----|
| Figure 3: Initiation Phase | 14 |
| Figure 4: Planning Phase..... | 15 |
| Figure 5: Conducting Phase | 21 |
| Figure 6: Reporting Phase..... | 26 |
| Figure 7: Closing Phase | 30 |

Acronyms

| | |
|-------|--|
| ATO | Authorization to Operate |
| CIO | Chief Information Officer |
| CIRC | Cyber Incident Response Capability |
| C-LAN | Classified Local Area Network |
| DOE | U.S. Department of Energy |
| EA | Office of Enterprise Assessments |
| EA-20 | Office of Cyber and Security Assessments |
| EA-21 | Office of Cyber Assessments |
| EACT | Enterprise Assessment Correspondence Tracker |
| FIE | Field Intelligence Element |
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Modernization Act |
| IARC | Information Assurance Response Center |
| IP | Internet Protocol |
| NIARC | NNSA Information Assurance Response Center |
| NIST | National Institute of Standards and Technology |
| NNSA | National Nuclear Security Administration |
| OFI | Opportunity for Improvement |
| PUB | Publication |
| QRB | Quality Review Board |
| RMA | Risk Management Approach |
| RMF | Risk Management Framework |
| ROE | Rules of Engagement |
| SSC | Support Services Contractor |
| SP | Special Publication |

Preface

The Office of Cyber Assessments (EA-21), within the Office of Enterprise Assessments (EA-1), is responsible for conducting independent cyber security assessment activities at U.S. Department of Energy (DOE) sites that possess high-value security interests as mandated in DOE Orders 227.1A, *Independent Oversight Program*, and 226.1B, *Implementation of Department of Energy Oversight Policy*.

The *EA-21 Assessment Process Guide* describes the processes, techniques, and procedures used by EA-21 to evaluate DOE's (including the National Nuclear Security Administration) and contractor organizations' cyber security programs designed to protect special nuclear material, classified information, and sensitive information. These evaluations are accomplished through the conduct of assessments that provide accurate, comprehensive information and analysis regarding the effectiveness of, and trends in, DOE programs and other functions of interest.

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 guide has been developed to be flexible and easily adaptable as it is applied during the various types of assessment activities. Use of this guide may also aid in the conduct of other DOE and contractor assessment activities. In order to ensure that this guide remains current and assessments continue to improve, all users of this guide are encouraged to provide comments and recommendations to EA-21 for consideration.

Definitions

Assessments – An assessment is an independent oversight activity conducted by the Office of Enterprise Assessments to evaluate the effectiveness of line management performance and risk management or the adequacy of DOE policies and requirements.

Best Practice – A best practice is a safety or security-related practice, technique, process, or program attribute observed during an appraisal 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 DOE field or Headquarters manager who is directly responsible for program management and direction, and the development and implementation of corrective actions. Cognizant managers may be line managers or managers of support organizations.

Deficiency – A deficiency is an inadequacy in the implementation of an applicable requirement or performance standard that is found during an assessment. Deficiencies may serve as the basis for one or more findings. In accordance with DOE Order 227.1A, *Independent Oversight Program*, EA-21 may use site- or program-specific equivalent nomenclature when assigning deficiencies and findings.

Directives - Directives are defined in DOE O 251.1, Departmental Directives Program.

Factual Accuracy – The process by which EA-21 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 which organization is responsible for corrective actions.

Opportunities for Improvement – Opportunities for improvement (OFIs) are suggestions offered in Enterprise Assessment (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. Opportunities for improvement 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 intended to be prescriptive or mandatory. Rather, they are suggestions offered by the EA review team that may assist site management in implementing best practices or provide potential solutions to minor issues identified during the conduct of the review. In some cases, OFIs address areas where program or process improvements can be achieved through minimal effort.

Major Vulnerability - A vulnerability which, if detected and exploited, could reasonably be expected to result in a successful attack causing serious damage to the national security.

Performance Testing - Activities conducted to evaluate all or selected portions of safety and security systems, networks, or programs as they exist at the time of the test. Performance testing includes, but is not limited to, force-on-force exercises, tabletop exercises, knowledge tests, limited-scope performance tests, limited-notice performance tests, penetration testing, vulnerability scanning, continuous automated scanning, and cyber security “red teaming.” Performance testing can be conducted as part of a scheduled appraisal activity (i.e., announced), or without prior knowledge of the entity being tested (i.e., unannounced).

Programmatic Reviews – Assessments that represent the combined evaluation of data collected during an assessment or cyber security review, which may include an examination of policy, procedures, and site-specific documents; the conduct of structured interviews with key personnel; the review of data centers, server rooms, and a sampling of workstations; and the overall assessment of the management, operations, and technical controls that implement the cyber security program for a selected DOE site office, contractor site, and headquarters organizations.

Recommendations – Recommendations are suggestions for senior line management’s consideration for improving program or management effectiveness. Recommendations transcend the specifics associated with findings, deficiencies, or opportunities for improvement and are derived from the aggregate consideration of the results of the assessment.

Red Team – A group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. The Red Team’s objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team. Definition derived from Committee on National Security System Instruction (CNSSI) 4009: CNSS Glossary.

Trusted Agent – An individual with appropriate operational authority or that has a compartmented role for coordination and conduct of EA-21’s scheduled, 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 conduct the test.

1.0 Introduction

The Department of Energy (DOE) Independent Oversight Program is implemented by the Office of Enterprise Assessments (EA). The Office of Cyber Assessments (EA-21), within EA, is responsible for conducting independent cyber assessment activities at DOE sites that possess high-value security interests, as mandated in DOE Orders 227.1A, *Independent Oversight Program*, and 226.1B, *Implementation of Department of Energy Oversight Policy*. EA-21 maintains its independence by having no direct responsibility for facility operations, protection program management, information systems management, or policy formulation.

1.1 Mission

The EA-21 mission is to independently evaluate the effectiveness of classified and unclassified cyber security programs throughout DOE. EA-21 accomplishes this by planning and conducting a variety of assessments that incorporate a broad range of threats to provide a complete and realistic evaluation of sites' cyber security postures. EA-21 is responsible for conducting assessments at DOE and National Nuclear Security Administration (NNSA) site offices and contractor sites. EA-21 develops and validates assessment results in reports that provide recommendations and identify findings, deficiencies, and opportunities for improvement. EA-21 also performs follow-up reviews to ensure site-specific corrective actions are effective.

This guide provides additional insight into the assessment approach and processes associated with assessing classified and unclassified cyber security programs. EA-21 cyber security activities encompass the following:

- Periodic assessments of classified and unclassified cyber security programs at DOE sites.
- Special reviews of classified matter protection and control programs.
- Periodic assessments of classified and unclassified cyber security intelligence programs at DOE sites.
- Remote testing for DOE network vulnerabilities through scanning and penetration testing.
- Unannounced penetration testing, commonly referred to as red teaming, of DOE sites.
- Follow-up activities to ensure that identified issues are addressed in a timely and effective manner.

-
- Studies of cyber security issues across the DOE complex.
 - Development of recommendations and identification of opportunities for improving cyber security performance.
 - Reviews of other governmental and commercial cyber security programs to provide benchmarks for DOE performance.
 - A “rapid response” capability to perform special reviews for the Secretary of Energy and senior DOE managers.
 - Ongoing analyses to identify trends and emerging issues in the cyber security arena.
 - Assessments of the effectiveness of DOE policies governing classified and unclassified cyber security.
 - Inputs for the annual evaluation of DOE’s classified information security programs and field intelligence elements (FIEs) as required by the Federal Information Security Modernization Act (FISMA).

In order to accomplish assigned responsibilities, EA-21 conducts various types of assessments that may include programmatic, technical, and special reviews.

1.2 Scope

The *EA-21 Assessment Process Guide* applies to EA-21 team members responsible for conducting cyber security assessments. This document serves as a primary resource to ensure consistency in completing an assessment. This guide will be reviewed and, if applicable, updated annually.

2.0 Applicable Laws, Orders, Policies, and Standards

The following laws and regulations establish security requirements to perform EA-21 assessments.

Table 1: Laws, Regulations, Policies, and Standards

| Laws, Orders, Policies, and Standards | |
|---|---|
| Laws and Regulations | <ul style="list-style-type: none"> • Federal Information Security Modernization Act of 2014 • The Privacy Act of 1974, Public Law 93-579 • Office of Management and Budget Circular A-130 • E-Government Act of 2002 • Computer Fraud and Abuse Act of 1986, Public Law, 99-474 (18 U.S.C. 1030) |
| DOE Orders | <ul style="list-style-type: none"> • DOE Order 205.1B, <i>Department of Energy Cyber Security Program</i>, March 11, 2013 • DOE Order 227.1A, <i>Independent Oversight Program</i>, December 2015 • DOE Order 226.1B, <i>Implementation of Department of Energy Oversight Policy</i>, April 25, 2011 |
| National Institute of Standards and Technology (NIST) Standards and Guidance | <ul style="list-style-type: none"> • NIST Special Publication (SP) 800-18 Revision 1 - <i>Guide for Developing Security Plans for Information Technology Systems</i>, February 2006 • NIST SP 800-30 - <i>Risk Management Guide for Information Technology Systems</i>, July 2002 • NIST SP 800-34 Revision 1 - <i>Contingency Planning Guide for Information Technology Systems</i>, May 2010 • NIST SP 800-37 Revision 1 - <i>Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach</i>, Feb. 2010 • NIST SP 800-53 Revision 4 - <i>Recommended Security Controls for Federal Information Systems and Organizations</i>, August 2013 • NIST SP 800-60 Revision 1 - <i>Guide For Mapping Types Of Information And Information Systems To Security Categories</i>, August 2008 • NIST SP 800-63 Version 1.0.2 - <i>Electronic Authentication Guideline</i>, April 2006 • NIST Federal Information Processing Standard (FIPS) Publication (PUB) 199 - <i>Standards for Security Categorization of Federal Information Systems</i>, February 2004 • NIST FIPS PUB 200 - <i>Minimum Security Requirements for Federal Information and Information Systems</i>, March 2006 |

Laws, Orders, Policies, and Standards

Committee on National Security Systems (CNSS)

- CNSSI 1253 - *Security Categorization and Control Selection for National Security Systems* March 2014
- CNSSI 1253F Attachment 1 - *Security Overlays Template*, August 2013
- CNSSI 1253F Attachment 2 - *Space Platform Overlay*, July 2013
- CNSSI 1253F Attachment 3 - *Cross Domain Solution Overlay*, September 2013
- CNSSI 1253F Attachment 4 - *Intelligence Overlay*, October 2012
- CNSSI 1253F, Attachment 5 - *Classified Information Overlay*, May 2014
- CNSSI 1253F, Attachment 6 - *Privacy Overlay*, April 2015

3.0 Governance

EA-21 is governed by the EA-21 Director. The EA-21 assessment team is comprised of Federal and support services contractor (SSC) staff. These staff members account for the programmatic and technical expertise maintained by this Office. The EA- Director is aligned with a contractor staff counterpart. Each Federal team member reporting to the EA-21 Director also serves as an Assessment Team Leader. While not depicted, each team member reports to their assigned leader (e.g. Programmatic Team Members to Programmatic Team Leader).

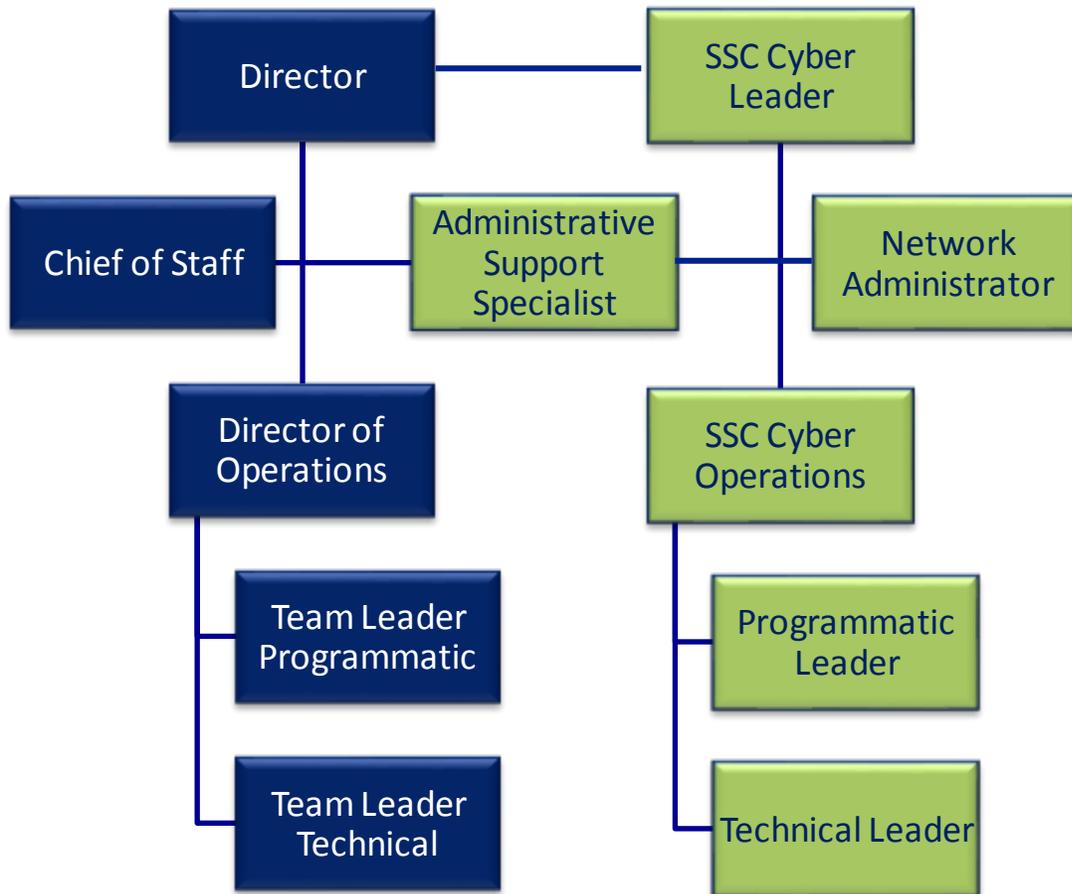


Figure 1: EA-21 Organizational Chart

3.1 Roles and Responsibilities

Each member of the EA-21 team serves as an integral part of the assessment lifecycle process. Table 2 lists the entities responsible for conducting assessment activities.

Table 2: Roles and Responsibilities

| Role | Responsibility |
|--------------------------------|--|
| EA-21 Director | <ul style="list-style-type: none"> • Provide overall direction for and management of the cyber security assessment program. • Provide DOE managers with an assessment of cyber security programs. • Brief senior DOE officials, including the Under Secretaries, Secretarial Officers, the EA Director, Director of Cyber and Security Assessments (EA-20), and DOE policy organizations, on the results of assessment activities. • Notify the EA-20 Director when assessment activities identify concerns that may have criminal or waste/fraud/abuse implications. • Develop and maintain topic assessor guides for conducting cyber security assessments. • Ensure that subsequent cyber security assessment activities review the effectiveness of corrective actions using a tailored approach based on significance and complexity. • Work with cognizant DOE line managers and policy organizations to resolve disagreements on assessment schedules, results, findings, or opportunities for improvement. • Participate in Quality Review Board (QRB) meetings. |
| Chief of Staff | <ul style="list-style-type: none"> • Ensure that the EA-21 Program activities are functioning as required. • Develop and maintain EA-21 policies, procedures, standards, and guides. • Respond to and participate in DOE data calls and strategic initiatives. |
| Director of Operations | <ul style="list-style-type: none"> • Direct and lead the overall activities of each Assessment Team Leader. • Participate in DOE data calls and strategic initiatives. • Designate assessment (inspection and review) team leaders. • Ensure the quality of assessment activities and reports. |
| SSC Cyber Leader | <ul style="list-style-type: none"> • Provide overall direction for and management of the cyber security assessment program support services contractors. |
| Assessment Team Leaders | <ul style="list-style-type: none"> • Provide direction and guidance consistent with the EA-21 Director. • Recommend assessment schedules. • Serve as Assessment Team Leader for inspections/reviews when designated by the EA-21 Director. • Support the EA-21 Director in interfacing with Headquarters and field personnel to coordinate activities and address concerns. • Recommend assessment team structure and scope. • Chair pre-QRB meetings. |

| Role | Responsibility |
|--|--|
| | <ul style="list-style-type: none"> • Participate in the QRB meetings. • Lead assessments of cyber security programs or topics. • Provide input on recommended assessment scope. • Provide direction and guidance to team members on the approach to specific assessment activities. • Draft cyber security Assessment Plans. • Provide feedback on proposed assessment team structure and make recommendations for additional resources needed to accomplish the scope. • Coordinate with the site for receipt of site documents prior to the assessment and for assessment logistics, as needed. • Establish the schedule of events for cyber security assessments. • Ensure that team members perform their assigned duties. • Address site concerns associated with assessment activities. • Provide feedback to site personnel daily to validate assessment information and clearly communicate areas of concern. • Oversee preparation and present assessment reports. • Brief site management and cyber security personnel on assessment results. |
| Programmatic and Technical Team Leaders | <ul style="list-style-type: none"> • Support Team Leader/Topic Team Leader in leading assessments of cyber security programs or topics. • Provide input on recommended assessment scope. • Provide direction and guidance to team members on the approach to cyber security programmatic activities or technical performance testing. • Provide input to the Team Leader/Topic Team Leader on document requests and other necessary logistics to support the assessment team. • Provide feedback on proposed cyber security assessment team structure and make recommendations for additional resources needed to accomplish scope. • Establish the cyber security assessment schedule and make specific assignments. • Ensure that team members perform their assigned duties. • Address site concerns associated with programmatic or technical performance testing activities. • Provide feedback to site personnel daily to validate assessment information and clearly communicate areas of concern. • Participate in briefing site management and cyber security personnel on assessment results, as required. • Prepare the programmatic and technical sections of the cyber security assessment report. • Work with the Team Leader/Topic Team Leader to resolve site comments on the assessment report. • Participate in pre-QRB meetings. • Participate in the QRB meetings. |
| Team Member(s) | <ul style="list-style-type: none"> • Support the Team Leader/Topic Team Leader and Programmatic or Technical Lead in conducting assessments of cyber security programs or topics. |

| Role | Responsibility |
|---------------------------------|--|
| | <ul style="list-style-type: none"> • Provide input to the Team Leader/Topic Team Leader and Programmatic or Technical Leader on assessment scope and potential approaches for accomplishing cyber security assessments. • Conduct assessment activities following direction and guidance of Team Leader/Topic Team Leader and the Programmatic or Technical Leader. • Assist in preparing the schedule of interviews to accomplish during onsite visit. • Review key site cyber security documents prior to the onsite visit (primarily a programmatic team function). • Execute external technical penetration tests and capture results prior to the site visit if included in the assessment scope (a technical team function). • Conduct thorough and fair assessments in accordance with the assessment plan. • Validate assessment data and conclusions with site personnel daily to ensure factual accuracy. • Participate in briefing site management and cyber security personnel on assessment results, if requested. • Provide written input for draft assessment reports, as directed by the Team Leader/Topic Team Leader and Programmatic or Technical Leader. • Work with the Programmatic or Technical Leader to resolve site comments on the assessment report. |
| Administrative Assistant | <ul style="list-style-type: none"> • Maintain the records repository for information and knowledge sharing in Enterprise Assessment Correspondence Tracker (EACT). • Collect and maintain an archive of information and data related to program management activities from the Cyber Assessment program. • Manage, control, and direct a physical records system, records organization and evaluation, and inactive records system. • Develop and maintain internal and external report correspondence. • Serve as travel coordinator. • Schedule QRB meetings. • Obtain conference call-in numbers. • Perform inter-office liaison. • Serve as parking reservation coordinator. • Maintain management calendars. • Coordinate all EA-21 office moves. • Coordinate staff meetings. • Record EA-21 Federal team members' time and attendance. |

4.0 Collaboration and Interfacing with External Organizations

EA-21 recognizes the value of collaborating and interfacing with other Headquarters program offices, field site offices, and DOE and NNSA site cyber security and information systems organizations to ensure that assessment results are clearly communicated and identified deficiencies are adequately addressed. EA-21 also works closely with the other EA offices and interfaces with organizations external to DOE, such as the White House, Congress, the Intelligence Community, and NIST.

4.1 Site Representatives

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

Relations between the assessment team and local representatives must be cordial, open, and professional to provide maximum value. EA-21 and the local representatives should approach cyber security assessments in partnership to ensure that these activities result in better protection levels for DOE information technology resources. This partnership 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. EA-21 also restricts the number of trusted agents to the minimum necessary to conduct testing. All trusted agents also sign a *Memorandum of Understanding and Agreement Regarding Trusted Agent Duties and Responsibilities* form prior to being briefed on sensitive test information. Finally, EA-21 shares performance test materials with trusted agents in person or, when necessary, by encrypted emails that provides the electronic signature of the trusted agent and cannot be forwarded.

5.0 EA-21 Assessment Teams

EA-21 assessments are comprised of technical and programmatic teams that include subject matter experts.

5.1 Technical Team

The EA-21 technical team conducts extensive internal and external performance testing to evaluate the effectiveness of protection measures for classified and unclassified networks. EA-21 uses this Assessment Process Guide to ensure a consistent technical approach to cyber security performance testing. This is an internal EA-21 document that defines internal and external performance testing, as well as information that is collected and retained during performance testing activities.

5.2 Programmatic Team

The EA-21 programmatic team focuses on both program direction and program implementation of the management, operations, and technical control components for analysis of overall effectiveness. Program direction is evaluated by assessing how well both DOE and contractor line management satisfies key responsibilities, and whether the resources, policies, and expectations for performance are adequate. Program implementation is evaluated based on whether the site policies and procedures are effectively and consistently implemented on site systems, periodically reviewed to ensure consistency with current DOE threat guidance and emerging technology, and sufficient to ensure that operational risks are identified, evaluated, and accepted by appropriate site DOE and contractor management.

6.0 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-21 has no responsibility for operations, projects, programmatic activities, budget, or policy development. EA-21 conducts a number of activities, collectively referred to as assessments, related to evaluating DOE policy and DOE and contractor line management performance in the areas under its purview. Dependent upon the scope of the assessment, these activities are generally grouped into two types: special reviews and assessments. Table 3 provides a list of assessment types performed by EA-21.

Table 3: Assessment Types

| Assessment Type | Description |
|------------------------|--|
| Assessment | Assess the effectiveness of one or more aspects of a site’s classified and/or unclassified cyber security program, as defined in the assessment scope. A focused assessment can include programmatic elements and/or less extensive technical performance testing. 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 and attending meetings. |
| Special Reviews | Conducted at the request of the Secretary or other senior DOE managers, often on a “rapid response” basis to provide specific needed information about DOE safety and security programs and policies, or other critical DOE functions. |

At the conclusion of each assessment, a validated report is published. The majority of reports will provide recommendations or opportunities for improvement for line management to consider as possible program enhancements. Reports may identify findings, which require corrective actions and high management attention. The reports may also list specific implementation deficiencies; suggested opportunities for improvement to assist cognizant managers in improving programs and operations; and any identified best practices that could help other DOE organizations solve challenging problems.

6.1 Assessment Testing Activities

Cyber security assessment processes are continually reviewed, refined, and applied according to the level of protection needed. Processes, procedures, and tools used are also adjusted, modified, and updated to remain current with the threats that new cyber technology introduces.

EA-21 has established a systematic approach for cyber security assessment activities 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 cyber security implementation. Performance testing provides a good snapshot of the effectiveness of performance but does not provide insight into the sustainability and direction of the program. Technical weaknesses that are identified through performance testing are generally symptoms of larger, more pervasive problems associated with management of the site's cyber security program. Therefore, EA-21 places significant emphasis on complementing technical performance testing with a programmatic review to assess the effectiveness of key underlying management processes associated with cyber security programs. This approach results in identification of systemic issues and provides a basis for evaluating the direction and sustainability of the associated cyber security programs.

6.1.1 Programmatic Assessments

During programmatic assessments, EA-21 evaluates the effectiveness of DOE cyber security policy through programmatic review at each site alongside technical performance testing. The team provides feedback to DOE's Office of the Chief Information Officer and, as relevant, to the NNSA Cyber Security Program Manager. EA-21 also evaluates DOE program office and site office performance as it relates to implementation of the cyber security programs. Programmatic assessments are conducted via data gathering, analysis of data call elements, and interviews with various site-, program-, or office-specific personnel.

6.1.2 Announced Penetration Testing

Announced penetration testing is typically conducted in conjunction with a scheduled unclassified cyber security assessment of a facility. Announced activities are primarily used to provide an overall assessment of a site's network security posture. These assessment activities are conducted remotely from EA-21's cyber security testing network facilities. EA-21 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.

6.1.3 Unannounced Penetration Testing

Unannounced penetration testing, also referred to as red teaming, is primarily used to evaluate a site's ability to withstand focused attacks from Internet sources. The key aspect to red teaming is that the site is not informed of the assessment beforehand. However, EA-21 does work with trusted agents at the site to coordinate activities and to assure that any areas of the site network that should be excluded from testing activities are known to the EA-21 team in advance.

6.1.4 Internal Penetration Testing

The key goal of internal penetration testing is to evaluate the strength of internal boundaries that provide isolation between differing need-to-know environments. Internal penetration testing is typically conducted during the onsite phase of announced assessments and may be applied to either classified or unclassified resources. Testing may be conducted using site-provided systems, EA-21 mobile assets, or a combination of both. EA-21 technical personnel are provided a 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 a red team activity, in which case such testing will be carefully coordinated with the trusted agent.

7.0 EA-21 Assessment Phases

All EA-21 assessments include five major phases: initiating, planning, conducting, reporting, and closing. Although these phases are identified as separate entities, some activities will occur during more than one phase of an assessment. Subsequent sections of this document, as well as the Assessment Plan constructed for each assessment (Section 7.2.5), describe the activities and expectations associated with each of the assessment phases. All EA-21 assessment templates described in the “output” tables of sections 7.1 – 7.5, are available on the EA [iPortal](#) in the “Assessment Templates” folder.



Figure 2: EA-21 Assessment Phases

7.1 Initiating

During the third quarter of each fiscal year (FY), the EA-21 Director, in conjunction with EA leadership, conducts internal planning sessions to determine which sites will be assessed during the following calendar year. This process involves stakeholders from across the DOE complex to inform them of the proposed sites that will undergo an assessment. Once an assessment schedule is established, the EA-21 Director prepares and sends a formal **Calendar Year Assessment Schedule Memo**.



Figure 3: Initiation Phase

7.1.1 Initiating Outputs

Table 4, lists the outputs from the **Initiating** phase of the assessment lifecycle.

Table 4: Initiating Outputs

| Output | Resources Needed | Responsible Party | Timeframe/Due Date |
|--------------------------------------|--|-------------------------------|--|
| Formal Calendar Year Assessment Memo | DOE stakeholder consensus | EA-21 Director | First quarter of the preceding fiscal year |
| Commence CNS reconnaissance | DOE Site's IP address range; CNS hardware/software | CNS Lead, Technical Team Lead | First quarter of the preceding fiscal year |

7.2 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 the site's or office's cyber security management, operations, and technical controls program.

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 and consists only of un-announced penetration testing requires less planning than a full assessment or a joint assessment with other EA offices.

Assessment activities scheduled by EA-21 are summarized in an Assessment Plan. This plan is sent to the site in advance of the scheduled assessment. When scheduling an assessment, one of the initial steps involves identifying and assigning resources for the activity. The EA-21 Director designates a Team Leader/Topic Team Leader and the Programmatic and Technical Leads. Working with the Programmatic and Technical Leaders, the Team Leader/Topic Team Leader plans the conduct of the assessment and closely coordinates with the EA-21 Director to ensure the thoroughness and rigor of the assessment.

The EA-21 Team Leader serves as the primary point of contact to DOE and contractor mid-level managers at the site. The EA-21 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. The Team Leader and Programmatic and Technical Leaders work with the EA-21 Director to develop, **Trusted Agent form, Document Requests (data calls), Assessment and Interview Schedules**, and the **Assessment Plan** that the EA-21 Director, and DOE Operations/Site Office representative sign. Team members are assigned to support the programmatic and technical aspects of the assessment as needed.

7.2.1 Planning Phase Activities

The EA-21 Director or the Team Leader initiates scoping and planning activities with the senior Federal or contractor site manager at least six to eight weeks prior the assessment 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.

The EA-21 team conducts a scoping visit, in-person or virtually, to become familiar with the site organization, reviews documentation, and develops an approach to the assessment. Onsite meetings or telephone conferences may be scheduled to assist in defining the scope of the upcoming assessment. Although a scope is established in the Assessment Plan, changing circumstances may warrant modifications; thus, flexibility should always be maintained. If included in the scope, EA-21 routinely begins external performance testing during the planning phase of the assessment after the ROE is signed. This allows the assessment team to collect critical performance testing data to support the programmatic and technical review during the conduct phase of the assessment. Scoping and planning activities include:

- Preparing and distributing the announcement memorandum, if one is required.
- Establishing assessment parameters.
- Reviewing available facility information (e.g., past reports, corrective action plans).
- Identifying assessment focus areas.
- Understanding the organizational structure and identifying key personnel to interview.
- Establishing site points of contact.
- Identifying cyber and FISMA systems that will be assessed.
- Logistics coordination with site personnel, including site access issues, training requirements, team space, and support needs.
- Preparing an Assessment Plan, including preliminary identification of systems/networks to be inspected, reviewed, or tested; development of preliminary programmatic assessment/review topics and interview schedules; ROE; and Trusted Agent forms).
- Developing 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.
 - Finalizing **travel logistics**.

Scoping or planning meetings may be conducted virtually or onsite. These meetings should occur at least six to eight weeks prior to the onsite assessment. These meetings allow assessment team members to meet key site personnel, review site documentation, conduct exploratory interviews, and determine how key areas can be assessed effectively.

7.2.2 Rules of Engagement

The ROE outlines the respective roles and responsibilities of the Office of Cyber Assessments staff, Federal and contractor site's cyber security 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 EA-21 Director and the designated Federal representative from the site must sign the Assessment Plan prior to beginning any performance 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 on the status of testing activities.
- Upon completion of testing, provide detailed information of the results to the site and coordinate with the site to return computer systems to the original configurations so that no systems are left in a compromised condition.
- In the unlikely event that performance testing adversely affects an information system, work with the site to determine the nature of the problem and restore the system to its desired state of operation.
- Inform the DOE integrated Joint Cybersecurity Coordination Center Cyber Incident Response Capability (iJC3) and the NNSA Information Assurance Response Center (IARC) of the start and stop dates of performance testing to ensure that testing activities are not confused with real attacks.

As part of establishing the ROE, the site is responsible for informing EA-21 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, EA-21 may exclude some cyber systems from performance testing activities. EA-21 also conducts a search for wireless access points controlled by that site that could allow access into the site's network.

7.2.3 Technical Data Call

To support cyber security performance testing, the EA-21 assessment team will request various documents at least six to eight weeks prior to the onsite assessment. The documents requested are due to EA-21 four weeks prior to the assessment. EA-21 traditionally requests the following types of technical data:

- Technical points of contact for network, computer systems, and telephone exchange systems; the point-of-contact data should include office telephone numbers, email addresses, and off-hour contact information.
- Internet protocol (IP) addresses for all site computers that include addresses exposed to the Internet, as well as any address ranges on restricted or "yellow" networks.
- 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 list of telephone phone numbers to be excluded and rationale as discussed above.
- A network topology map containing perimeter devices and IP addresses of those devices, including main border router, other routers, that have separate Internet connections, firewalls, gateways, and major subnet routers.
- Router access control lists, firewall rules, and intrusion detection/prevention rules.
- Information related to any wireless networks in use to include Service Set Identifier (SSID) and Media Access Control (MAC) addresses of all authorized access points.
- Diagrams of the classified and unclassified computer network(s).

7.2.4 Programmatic Review Data Call

The EA-21 assessment team requests documents from the site at least six to eight weeks prior to the onsite assessment. The documents requested are due to EA-21 four weeks prior to the assessment. Document requests typically include:

- Organization charts, including names and telephone numbers of individuals with a role in the site's cyber security program, and primary points of contact for team members.
- The current Program Cyber Security Plan and Cyber Security Program Plan used for cyber security management, and other relevant site-specific management documents.
- Site cyber security policies and procedures.

-
- The current Program Office Risk Management Approach (RMA) Implementation Plan appropriate to the site, and any site Risk Management Framework (RMF) documentation describing how the site is implementing the RMA/RMF.
 - Site's current 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).
 - Site-specific threat assessment information.
 - Site-specific risk assessments.
 - A list of computers and networks that process classified and sensitive unclassified information (e.g. Unclassified Controlled Nuclear Information, Official Use Only), including accreditation or authority to operate (ATO) dates. ATO documents for systems included in the assessment or review scope should be requested once those systems are identified by the assessment team.
 - Security plans or master plans that describe the cyber security protection measures for computer systems, including related certification testing documents, business impact assessments (BIAs), privacy impact assessments (PIAs), contingency plans, and risk assessments for those systems included in the assessment or review scope.
 - Copies of recent (within the last two years) assessments, surveys, self-assessments, and reviews for classified and unclassified cyber security programs.
 - Issue tracking reports, corrective action plans, Plan of Action and Milestones reports.
 - Results of the most recent site external and internal vulnerability scans (for coordination with the technical team).
 - A list of cyber security incident reports for classified and unclassified systems over the past two years.
 - Identification of the DOE cyber security directives contained in the contracts for each of the site's contractors who manage the IT and/or Cyber Security programs and associated assets.

7.2.5 Assessment Plan

For each assessment, EA-21 develops 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 EA-21 conducts joint assessment activities, a joint Assessment Plan will be developed by the Team Leader, with input from the EA-21 Topic Team Leaders. Although EA-21 is not limited to evaluating specific areas in the Assessment Plan, every effort is made to identify areas of emphasis during the assessment. A copy of the Assessment Plan, once approved by the EA-20 Director, is sent to the site prior to the onsite assessment.

7.2.6 Onsite Assessment Schedule

The assessment schedule is designed to efficiently use the limited time on site and 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 EA-21 assessment team will prepare slides for the beginning and closing of the overall assessment. The **in-brief slides** will provide a brief overview of the assessment scope, schedule, and activities alongside a site in-brief that provides an overview of the operations and mission at the site.

The EA-21 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. Additionally, a management meeting with the senior site management (e.g., security director, the chief information officer) may be held each day to briefly discuss the progress of the programmatic review and performance testing.

7.2.7 Planning Outputs

Table 5, lists the outputs from the **Planning** phase of the assessment lifecycle.

Table 5: Planning Outputs

| Output | Resources Needed | Responsible Party | Timeframe/Due Date to/from Site |
|---|---|--|-----------------------------------|
| Scoping and Planning Call or In-person Meeting | EA-21 Team Leader, Technical and Programmatic Leaders, and Site/Program Office Stakeholders | Assessment Team Leader | 6-8 weeks prior to the assessment |
| Assessment Plan (to include site points of contact) | Assessment Plan Template; Document Request Template | EA-20 Director and Assessment Team Leader | 6-8 weeks prior to the assessment |
| Site returns data call | <ul style="list-style-type: none"> Feedback from the site | Assessment Team Leader | 4 weeks prior to the assessment |
| Logistics and travel plans (normally documented in a memo sent to team members) | Concur | EA-21 Director, Assessment Team Leader, and Administrative Assistant | 4 weeks prior to the assessment |
| Deliver CNS results to | CNS reconnaissance | CNS Lead, | 4 weeks prior to the |

| Output | Resources Needed | Responsible Party | Timeframe/Due Date to/from Site |
|--|--|-------------------------|---------------------------------|
| technical team | results | Technical Team Lead | assessment |
| Completion of site required training and application for physical/logical access | Site supplied forms and training materials/instructions | Assessment Team Members | 3 weeks prior to assessment |
| Visitor requests submitted and accepted by site | Site visitor request forms, training certificates | EA Admin and Site FSO | 3 weeks prior to assessment |
| Completed Assessment and Onsite Interview Schedule sent to team and site | Information garnered from data calls | Assessment Team Leader | 2 weeks prior to the assessment |
| Signed Trusted Agent Form | Trusted Agent Template | Assessment Team Leader | 1 week prior to the assessment |
| Send iJC3 notification (for external assessments) | iJC3 Notification Email Template | Assessment Team Leader | 1 week prior to assessment |
| Commence external scanning of the site provided IP ranges | Scanning hardware and software | Technical Team | 1 – 2 weeks prior to assessment |
| Site Logistics email to team | Site Address/Map; Latest Site Documents; Weather forecast for area; Assessment Schedule; Hotel Address/Map | Assessment Team Leader | 2-4 days prior to assessment |
| Final In-Brief Slides sent to team and site | In-Brief/Closeout briefing Template | Assessment Team Leader | 1 week prior to assessment |

7.3 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 cyber security programs, thus allowing a reasonable judgment of protection effectiveness.

To gain insight into a site's cyber security programs, and to understand interdependencies with other site activities, EA-21 uses a "bottom-up" approach to program assessment. As a first step, unclassified cyber security assessments may begin with extensive external and internal network performance testing that might include an initial site visit several weeks prior to the programmatic review (i.e., during a planning visit). Performance testing, including attempts to penetrate the site's network, is also conducted remotely over the Internet from EA-21's Cyber Security Testing Networks. EA-21 may also conduct tabletop reviews of computer systems excluded from performance testing, firewall rules, and intrusion detection systems to fully assess the protection provided by the network. As noted in the Planning Section, EA-21 will review any site request and site justification for exclusion of certain critical safety or operational systems from testing as part of the process of developing the ROE.

During the Conducting phase of the assessment, EA-21 conducts performance testing and performs a programmatic review to evaluate essential underlying management processes. This phase includes intense and varied activities, such as interviews, walkthroughs, tabletop reviews, and data analysis that are customized to accurately assess the site's ability to protect its classified and unclassified networks. During this stage, EA-21 develops assessment conclusions based on analysis of data, and validates information with site personnel.

7.3.1 Technical Review

The approach to the technical review, or sometimes referred to as performance testing activities, is a key element of EA-21 cyber security assessments because it provides tangible feedback on the current effectiveness of a site's cyber security protection posture. 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. EA-21 technical team members plan and conduct performance testing based on this knowledge and the characteristics of the site resources. 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.

However, performance testing by itself does not allow for valid conclusions on the direction or sustainability of the program. A programmatic review is conducted to assess the effectiveness and stability of the program and to evaluate essential management processes that form the foundation for the cyber security program. Performance testing results are also used as input for the programmatic review to identify specific weaknesses (symptoms) so that underlying causes or root causes of systemic problems can also be identified. The combination of extensive performance testing and a review of essential program elements allows EA-21 to fully and effectively assess unclassified and classified cyber security programs.

Any misuse of computer systems detected during performance testing is reported immediately to site management. If criminal activity is suspected, EA-21 reports this information to the Office of

the Inspector General for investigation and resolution. EA-21 does not investigate alleged criminal activity or misconduct. The site is responsible for reporting computer security incidents to program officials, iJC3, and other organizations, as appropriate. Likewise, EA-21 is responsible for coordinating the performance testing activities with iJC3.

7.3.2 Programmatic Review

The programmatic team conducts interviews with federal and contractor cyber security and IT personnel, reviews new or revised documentation not submitted with the data call, confirms cyber security 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 program performance is consistent with site policies or to identify elements where performance deviates from policies and standards.

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 cyber security 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.

7.3.3 Communication and Feedback

EA-21's objective throughout each assessment activity is to ensure that a thorough and accurate assessment of a site's cyber security program is conducted and that site personnel gain maximum benefit from the experience. To accomplish this, EA-21 personnel, site managers, and site cyber security staff must all communicate extensively. This communication begins prior to the onsite assessment activities and continues throughout the assessment lifecycle. During the first day of the assessment, the Team Leader/Topic Team Leader briefs site personnel on the anticipated scope, onsite schedule, and report preparation process. Onsite cyber security personnel typically follow this initial briefing with an overview of the site's program, resources, and any changes that have occurred since the planning meetings or the last inspection. 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, EA-21 personnel provide routine feedback to the site on the progress of the assessment, keeping site personnel informed of any potential concern associated with the review. The site being appraised has an opportunity and responsibility to provide feedback to EA-21 personnel when concerns over factual accuracy exist. The site should provide additional data and identify site personnel who can help EA-21 personnel identify corrections for any factual accuracy misunderstanding. The following activities are integrated into the EA-21 assessment process to ensure that the assessment team and site managers and staff have an opportunity to effectively communicate.

- Remote performance testing - EA-21 technical personnel are in contact with site personnel routinely to discuss the status of testing and any issues.
- Onsite programmatic and technical team review activities – the EA-21 assessment team will schedule a daily informal validation meeting with site cyber security staff to provide feedback on the progress of data collection, areas requiring further review, and issues of potential concern, if any. **Daily validation meetings** with the site/program office are held at the beginning of each day. The daily validations should focus on what program elements were addressed, what technical activities and tests were performed, and a summary of the results of those interviews, document reviews, and testing processes.
 - A meeting is held daily with the Assessment Team Leader (or Team Leader/Topic Team Leader) and appropriate managers to provide a management perspective on the progress of the programmatic review and performance testing.
 - Site management should be informed of cyber security assessment progress and issues by the site cyber security staff attending the daily validation meetings. This is not primarily an EA-21 responsibility unless a significant vulnerability is identified by the assessment team, such as a serious technical vulnerability or discovery of an in-progress cyber-attack, in which case it is incumbent on the EA-21 Assessment Team Leader/Topic Team Leader to immediately notify site management.
 - Informing EA management of key results is the responsibility of the EA-21 Team Leader/Topic Team Leader and is based on the daily validation meeting content. Discovery of a serious technical vulnerability or discovery of an in-progress cyber-attack should immediately be reported to EA management concurrent with reporting the situation to site management.
- **Pre-decisional Closeout Briefings** - Provided to key managers at the conclusion of an assessment. The Assessment Team Leader, EA-21 Director, or Team Leader/Topic Team Leader presents the pre-decisional results of the assessment to the key DOE field and contractor line managers, highlighting program strengths, any identified findings, and areas for improvement related to the site's classified and unclassified cyber security programs. The final validation during the closeout briefing should be limited to a high-

level summary of scope and pre-decisional results, given that more detailed validation meetings with site personnel were held during the assessment period and that more senior management usually attend the closeout briefing. For external network security assessments that are conducted remotely, the EA-21 Director and Team Leader/Topic Team Leader will travel to the site (or arrange a conference call) after receiving factual accuracy feedback on the initial draft report, in preparation for briefing site management on the results.

Periodically, sites ask for feedback on their approach to implementing cyber security measures or request recommendations regarding products to use. As part of its effort to help DOE sites, EA-21 is open to conducting a dialogue on technical issues. **As an Office of Cyber Assessments organization, EA-21 does not direct a site to take any specific action, use any specific cyber security tools, or adopt any specific technical solutions.** Rather, EA-21 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 is a line management responsibility.

7.3.4 Conducting Outputs

Table 6, lists the outputs from the **Conducting** phase of the assessment lifecycle.

Table 6: Conducting Outputs

| Output | Resources Needed | Responsible Party | Timeframe/Due Date |
|----------------------------------|---|---|---|
| Daily Validation Meetings | Daily onsite input from the EA-21 programmatic and/or technical team | Assessment Team Leader and programmatic and/or technical Team Leaders | Daily |
| Pre-decisional Closeout Briefing | Consolidated daily onsite input from the EA-21 programmatic and/or technical team | Assessment Team Leader and programmatic and/or technical Team Leaders | Five business days after the assessment |

7.4 Reporting



Figure 6: Reporting Phase

The goal of the Reporting phase is to thoroughly analyze all available data and draw valid conclusions in order to prepare an assessment report, prepare the report, and inform site management of results. Reports are sent to EA-1 for concurrence within 60 days of completion of onsite assessment activities.

7.4.1 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 cyber security program, as well as underlying root causes for that condition. The goal of analysis is to have logical, supportable conclusions that portray a fair picture of how well a cyber security program functions to protect classified and unclassified DOE information and technology resources. All team members work closely during this phase to ensure that all information and points of view are considered.

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

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

7.4.2 Findings, Deficiencies, Recommendations, and Opportunities for Improvement

Findings are used to document specific significant weaknesses identified during assessment activities associated with protection of information technology resources or essential underlying management processes that support the program. A finding is a deficiency that warrants 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 which organization is responsible for corrective actions. The Team Leader/Topic Team Leader is responsible for recommending the findings that should be assigned to a site's cyber security program as the result of an assessment.

Deficiencies are an inadequacy in the implementation of an applicable requirement or performance standard that is found during an appraisal. Deficiencies may serve as the basis for one or more findings.

OIs are suggestions offered in Independent Oversight appraisal reports that may assist cognizant managers in improving programs and operations. While they may identify potential solutions to findings and deficiencies identified in appraisal reports, they may also address other conditions observed during the appraisal process. Opportunities for improvement are provided only as recommendations for line management consideration; they do not require formal resolution by management through a corrective action process.

7.4.3 Report Preparation

A report is issued to formally document the results of assessment activities and is intended for dissemination to the Secretary, appropriate DOE managers at Headquarters and in the field, and site contractors.

The cyber security assessment report is prepared following the report format designated by EA-21. The programmatic and technical team leaders, in coordination with the EA-21 team leader, are responsible for preparing the draft assessment report. The programmatic team leader has responsibility for the overall report and assigns responsibility for writing various programmatic sections of the report to the other programmatic team members. The technical team leader has overall responsibility for the technical sections of the report, assigns responsibility for writing individual technical sections to the other technical team members, and is responsible for providing the technical results section to the programmatic team leader for inclusion in the final draft assessment report. Reports for assessments that only include one aspect of the cyber security program (e.g., only programmatic elements or only technical elements) are prepared by the designated programmatic or technical team leader, with writing responsibilities assigned to other team members as needed.

Every effort should be made to ensure that the report contents are unclassified. If there are any questions regarding the classification of a planned section or result, the team members should consult, in a secure manner, with an EA-authorized derivative classifier *prior to* writing. If the decision is that the intended content is classified, that portion of the report must be written on an accredited EA system, preferably on the Headquarters classified local area network (C-LAN). Once the (unclassified) balance of the assessment report is prepared, the unclassified report should be uploaded to C-LAN following established transfer procedures, and the classified sections incorporated into the final draft 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 that have been collected and information that has been validated during the “conducting phase” of the assessment.
- The respective Federal Team Leader and SSC VP reviews the draft report prior to the formal editorial process.
- The QRB reviews the draft report to ensure that it is readable, logical, and contains adequate, balanced information to support the conclusions.
- DOE and site contractor personnel are given the opportunity to review draft reports for factual accuracy. EA-21 typically 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 on which the site has a comment related to factual accuracy. Formal factual accuracy comments from the site are due five working days after receipt of the draft report. EA-21 team members review all factual accuracy comments, and changes are made to the report, as appropriate. Factual accuracy reviews are not intended to allow site reviewers to eliminate conclusions or findings that the site or managers view as unfavorable, nor are the factual accuracy reviews intended to allow the site to provide progress reports or changes in status that occurred since the assessment was conducted. The assessments are clearly 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 factual accuracy reviews.

7.4.4 Pre Quality Review Board Meeting

After the draft copy of the report is sent to the QRB members and their comments are collected by the Administrative Assistant, the assessment team will hold a pre-QRB meeting to discuss the comments and determine a team response or corrective action. This meeting is chaired by the

Assessment Team Leader.

7.4.5 Quality Review Board

The QRB reviews draft reports from a leadership perspective. The QRB provides feedback on the readability of the report, whether or not the analysis and conclusions are appropriately supported, and whether the standards applied are consistent with other EA assessment activities. The QRB is chaired by the Deputy Director of EA-1 and includes the EA-21 Director and other senior personnel as directed.

7.4.6 Report Distribution

Once the draft review reports have been revised to reflect comments and suggestions from the QRB, the report is distributed to the site and responsible program office. Final assessment reports are transmitted via memorandum from the EA-20 Director and sent to the DOE/NNSA site office Manager, the site Chief Information Officer (CIO), and the senior executive of the responsible program office at Headquarters. This process is generated by the EA-21 Administrative Assistant via EACT for report distribution and approval. Reports for are transmitted via email by the EA-21 Director and sent to the DOE/NNSA site office Manager, the site CIO, and the senior executive of the responsible program office at Headquarters. Reports for special reviews are transmitted via memorandum from the EA Director and sent to the DOE/NNSA site office Manager, the site CIO, the senior executive of the responsible program office at Headquarters, and others as deemed appropriate. Reports for FIE assessments are transmitted via memorandum from the EA Director to the Office Director, National Intelligence, and the Director, Office of Intelligence and Counterintelligence.

Within three days of the final report dissemination, the unclassified report title will be posted to the EA Website in accordance with the EA Operational Plan, unless otherwise directed.

7.4.7 Reporting Outputs

Table 7, lists the outputs from the **Reporting** phase of the assessment lifecycle.

Table 7: Reporting Outputs

| Output | Resources Needed | Responsible Party | Timeframe/Due Date |
|-------------------------|---|------------------------|---|
| Draft Assessment Report | <ul style="list-style-type: none">Daily onsite input from the EA-21 programmatic and/or | Assessment Team Leader | 30 days after the conclusion of the onsite assessment |

| Output | Resources Needed | Responsible Party | Timeframe/Due Date |
|--|--|--|--|
| | technical team.; Analytical data gathered during the onsite assessment activities. | | |
| Final Assessment Report | Concurrence on QRB and site comments | Assessment Team Leader, Administrative Assistant, and Eagle Research Group (ERG) Cyber Team Leader | 60 days after the conclusion of the onsite assessment |
| Report Distribution | Final Report EACT | Administrative Assistant | 75 - 90 days after the conclusion of the onsite assessment |
| Post Unclassified Report Title to EA Website | Report title Posting process | Administrative Assistant | 3 business days following report dissemination |

7.5 Closing



Figure 7: Closing Phase

The **Closing** phase includes all the activities necessary for the Team Leader to close the assessment. It is important that lessons learned during the assessment are captured and that information is properly archived. This phase marks the end of the assessment process until the team moves to the next site or program to begin the Initiating phase again.

7.5.1 Process Improvements

EA-21 supports the concept of continuous improvement in order to make cyber security assessments more effective and of value to DOE sites, departmental managers, and other stakeholders. The Team Leader/Topic Team Leader is responsible for soliciting feedback from each team member and making recommendations to the EA-21 Director on process improvements.

EA-21 also solicits feedback from DOE field and contractor line managers to ensure that the assessment process provides value to site personnel. EA-21 welcomes any feedback on how

assessment processes can be improved.

7.5.2 Documentation of Assessment Activities

EA-21 assessment team members collect a large volume of data and information through performance testing, document reviews, and interviews. EA-21's 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, considering that EA-21's mission is to conduct the annual evaluation of DOE classified information technology systems and to provide input to the annual evaluation of DOE unclassified information technology systems as required by FISMA and DOE Orders 227.1A, 226.1B, and 205.1B. Each member of an EA-21 assessment team has a role in documenting assessment activities for use in the development of conclusions. The EA-21 Team Leader/Topic Team Leader is responsible for ensuring that key assessment information is captured and retained in a formal **Lessons Learned** document.

EA-21 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 classified interview sheets or performance testing results that are retained. To prevent managing large quantities of paper documents, a high-speed scanner will be used to convert information to electronic format so it can easily be stored on electronic media, encrypted at rest. All assessment documentation that is retained will be for internal use only, except as authorized by the EA-21 Director in support of IG audits and other valid reasons.

7.5.3 Records Retention

EA-21 maintains copies of the following documents in the file repository, EAShare, for each assessment activity.

- **Signed Site Assessment Plan**
- **Onsite in-briefs and pre-decisional closeout briefings**
- **Report comments matrix**
- **Final report**

7.5.4 Closing Outputs

Table 8, lists the outputs from the **Closing** phase of the assessment lifecycle.

Table 8: Closing Outputs

| Output | Resources Needed | Responsible Party | Timeframe/Due Date |
|---|---|------------------------|-------------------------------|
| Final copies of documents listed in Section 7.5.3 | EA Share | Assessment Team Leader | 30 days after report issuance |
| Lessons Learned Document | EA-21 Assessment Team Institutional knowledge | Assessment Team Leader | 60 days after report issuance |

Appendix A: Assessment Program Outputs

All EA-21 assessment templates are available on the EA [iPortal¹](#) in the “Assessment Templates” folder.

Table 9: EA-21 Assessment Program Outputs

| Phase | Output | Resources Needed | Responsible Party | Timeframe/Due Date to/from Site |
|------------|--|---|-------------------------------|--|
| Initiating | Formal Calendar Year Assessment Memo | DOE stakeholder consensus | EA-21 Director | First quarter of the preceding fiscal year |
| | Commence CNS reconnaissance | DOE Site’s IP address range; CNS hardware/software | CNS Lead, Technical Team Lead | First quarter of the preceding fiscal year |
| Planning | Scoping and Planning Call or In-person Meeting | EA-21 Team Leader, Technical and Programmatic Leaders, and Site/Program Office Stakeholders | Assessment Team Leader | 6-8 weeks prior to the assessment |

¹ iPortal access URL:

https://iportalwc.doe.gov/webcenter/portal/oracle/webcenter/page/scopedMD/s8bba98ff_4cbb_40b8_bee6_296c916a23ed/businessRolePages/GroupSpaceDocLibMainView.jspx?wc.contextURL=%2Fsaces%2FEA_21&adf.ctrl-state=m2jky1vgg_332&afLoop=748507340384105#!%40%40%3F%2FafLoop%3D748507340384105%26wc.contextURL%3D%252Fsaces%252FEA_21%26%2Fadf.ctrl-state%3Dzvehz19yh_76

| Phase | Output | Resources Needed | Responsible Party | Timeframe/Due Date to/from Site |
|-------|--|---|--|-----------------------------------|
| | Assessment Plan (to include site points of contact) | Assessment Plan Template; Document Request Template | EA-20 Director and Assessment Team Leader | 6-8 weeks prior to the assessment |
| | Site returns data call | Feedback from the site | Assessment Team Leader | 4 weeks prior to the assessment |
| | Logistics and travel plans (normally documented in a memo sent to team members) | Concur | EA-21 Director, Assessment Team Leader, and Administrative Assistant | 4 weeks prior to the assessment |
| | Deliver CNS results to technical team | CNS reconnaissance results | CNS Lead, Technical Team Lead | 4 weeks prior to the assessment |
| | Completion of site required training and application for physical/logical access | Site supplied forms and training materials/instructions | Assessment Team Members | 3 weeks prior to assessment |
| | Visitor requests submitted and accepted by site | Site visitor request forms, training certificates | EA Admin and Site FSO | 3 weeks prior to assessment |
| | Completed Assessment and Onsite Interview Schedule sent to team and site | Information garnered from data calls | Assessment Team Leader | 2 weeks prior to the assessment |
| | Signed Trusted Agent Form | Trusted Agent Template | Assessment Team Leader | 1 week prior to the assessment |
| | Send JC3 notification (for external assessments) | JC3 Notification Email Template | Assessment Team Leader | 1 week prior to assessment |
| | Commence external scanning of the site provided IP ranges | Scanning hardware and software | Technical Team | 1 – 2 weeks prior to assessment |

| Phase | Output | Resources Needed | Responsible Party | Timeframe/Due Date to/from Site |
|------------|---|--|--|--|
| | Site Logistics email to team | Site Address/Map; Latest Site Documents; Weather forecast for area; Assessment Schedule; Hotel Address/Map | Assessment Team Leader | 2-4 days prior to assessment |
| | Final In-Brief Slides sent to team and site | In-Brief/Closeout briefing Template | Assessment Team Leader | 1 week prior to assessment |
| Conducting | Daily Validation Meetings | Daily onsite input from the EA-21 programmatic and/or technical team | Assessment Team Leader and programmatic and/or technical Team Leaders | Daily |
| | Pre-decisional Closeout Briefing | Consolidated daily onsite input from the EA-21 programmatic and/or technical team | Assessment Team Leader and programmatic and/or technical Team Leaders | Last day of the assessment |
| Reporting | Draft Assessment Report | Daily onsite input from the EA-21 programmatic and/or technical team.; Analytical data gathered during the onsite assessment activities. | Assessment Team Leader | 30 days after the conclusion of the onsite assessment |
| | Final Assessment Report | Concurrence on QRB and site comments | Assessment Team Leader, Administrative Assistant, and Eagle Research Group (ERG) Cyber Team Leader | 60 days after the conclusion of the onsite assessment |
| | Report Distribution | Final Report EACT | Administrative Assistant | 75 - 90 days after the conclusion of the onsite assessment |

| Phase | Output | Resources Needed | Responsible Party | Timeframe/Due Date to/from Site |
|---------|---|---|--------------------------|--|
| | Post Unclassified Report Title to EA Website | Report title Posting process | Administrative Assistant | 3 business days following report dissemination |
| Closing | Final copies of documents listed in Section 7.5.3 | EA Share | Assessment Team Leader | 30 days after report issuance |
| | Lessons Learned Document | EA-21 Assessment Team Institutional knowledge | Assessment Team Leader | 60 days after report issuance |