U.S. DEPARTMENT OF
ENERGY

Enterprise Assessments

Office of Cyber Assessment Strategy

Concept of Operations

March 2022

Version 2.0

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
Version 1.0	EA-61 Advisory Group	03/2020	Initial release.
Version 2.0	Lewis, McFearin	03/2022	Updates for FY22

Office of Cyber Assessment Strategy
Concept of Operations

Approval Form

CHRISTOPHER MCFEARIN
Digitally signed by CHRISTOPHER MCFEARIN
Date: 2022.03.24 12:50:03 -06'00'

Approved by: ______________________
Christopher E. McFearin
Acting Director
Office of Cyber Assessments
Office of Enterprise Assessments

Joseph Lewis, Sr.
Digitally signed by Joseph Lewis, Sr.
Date: 2022.03.24 12:49:49 -05'00'

Acknowledged by: ______________________
Joseph Lewis
Director
Office of Cyber Assessment Strategy
Office of Enterprise Assessments

Table of Contents

1. Introduction

Purpose

This Concept of Operations (CONOPS) defines the functions of the Office of Cyber Assessment Strategy (EA-61) to ensure it is aligned with the Office of Cyber Assessments (EA-60) and DOE mission priorities, responds to emerging threats, and provides effective knowledge management (KM) and knowledge development (KD) support.

This CONOPS is a living document and will be reviewed annually. The approved version of this document will be available on the Energy.gov website. To ensure that this document remains current, team members are encouraged to provide comments and recommendations to the EA-61 Director for consideration.

Authorities and Governance

The DOE Independent Oversight program is implemented by the Office of Enterprise Assessments (EA), according to the requirements established in DOE Policy 226.2, *Policy for Federal Oversight and Contractor Assurance Systems*, which establishes the expectation for the implementation of a comprehensive and robust oversight process that enables the Department's mission to be accomplished effectively, efficiently, safely, and securely; and DOE Order 227.1A, *Independent Oversight Program*, which identifies EA-60 as the organization responsible for conducting cybersecurity assessment activities for DOE sites and facilities. In addition, EA-60 conducts assessments of DOE and National Nuclear Security Administration 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.

Each year, the EA fiscal year (FY) Operational Plan is approved by the Director and Deputy Director of EA and outlines the mission, vision, and values of the organization and prescribes the priorities to be addressed by EA-60. In FY 2022, EA-60 will work to ensure implementation and compliance with Federal guidance and key mandates that are released or updated. These mandates and guidance are listed in Appendix C, *Legislation, Federal Directives, and Mandates*.

Mission

EA-61 is responsible for the development and management of information identified from assessments and analysis of cybersecurity trends to enhance the overall effectiveness of cyber assessments. This information provides effective decision support information for cybersecurity leaders to use in evaluating cybersecurity strategies and plans across the Department.

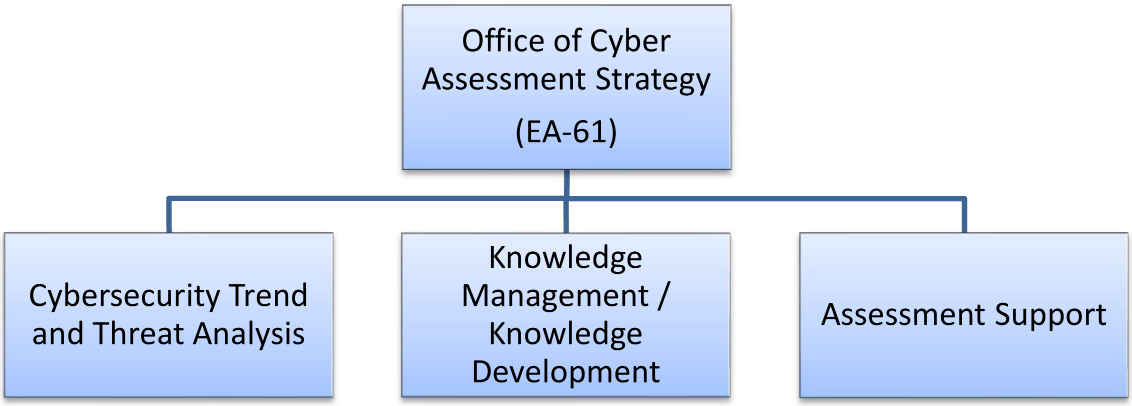
EA-61 KM and KD functions include the research and correlation of cybersecurity information relevant to DOE and EA-60 assessments into reports. These reports may include threat information, assessment site profiles, relevant cybersecurity incidents, site cybersecurity conditions, emerging cybersecurity requirements, and other relevant information to enable more effective review of cybersecurity programs across the Department. EA-61 is also responsible for development and implementation of the required information sharing infrastructure to facilitate improved knowledge sharing and reporting.

2. Organizational Overview

Office of Cyber Assessment Strategy (EA-61)

As cyber threats continue to increase and evolve, EA-61 must ensure that it can effectively support the assessment process of cybersecurity programs with timely, relevant, and useful information regarding cybersecurity trends, threats, and emerging requirements. In support of this mission, EA-61 is divided into three main functions: Cybersecurity Trend and Threat Analysis, Knowledge Management / Knowledge Development, and Assessment Support.

Figure 1 depicts the EA-61 functions.



Office of Cyber Assessment Strategy (EA-61)

Cybersecurity Trend and Threat Analysis

Knowledge Management / Knowledge Development

Assessment Support

Figure 1: EA-61 Functions Chart

Each team member of EA-61 serves as an integral part of the strategy functions. Table 1 lists the major functions that each team member will support executing strategy deliverables.

Table 1: EA-61 Functions

Function	Responsibility
EA-61 Director	• Work with the EA-60 Director and Office of Cyber Assessment Operations (EA-62) Director to define and integrate assessment strategies that align with DOE mission priorities. • Oversee and maintain the EA-60 KM and KD efforts. • Create, manage, and maintain collaborative partnerships with key stakeholders to provide timely, relevant, and useful information on cyber trends, threats, and assessments.
Cybersecurity Trend and Threat Analysis	• Identify, analyze, and catalog cybersecurity trends, threats, vulnerabilities, and other relevant information to inform the assessment process. • Make informed recommendations to EA-60 and EA-62 personnel for inclusion into the assessment process, both programmatic and technical, by utilizing relevant cybersecurity trends, threats, vulnerabilities, or other relevant information.
Knowledge Management / Knowledge Development	• Create and maintain information-sharing infrastructure to facilitate KM and KD efforts. • Establish and maintain a process for identifying, analyzing, and describing emerging cybersecurity trends and threats. • Create, maintain, and share a catalog of timely, relevant, and useful cybersecurity threat and trend information within EA-60, EA, and the Department. • Use post-assessment lessons learned to inform strategic decision making, future assessments, and process improvement efforts. • Represent EA and EA-60 on working groups, integrated project teams, and other collaborative efforts to provide cybersecurity subject matter expertise across the Department.
Assessment Support	• Create and maintain site profiles and site profile addendums for every assessment per timelines outlined in the Assessment Process Guide.

	• Tailor site profile addendums to site mission to inform the assessment process with timely, relevant, and useful information. • Gather, catalog, and analyze post-assessment lessons learned for KM and KD efforts. • Receive, process, and arbitrate new Federal requirements, DOE Directives, Policy, and other official guidance to make recommendations for inclusion into the assessment process.

3. Strategy Process

Strategy drivers can originate from different sources internal and external to the EA-61 organization. EA-61 assesses these drivers and in coordination with the EA-60 and EA-62 Directors develops applicable protocol, processes, or capabilities to meet the strategic needs of the EA-60 organization.

Cybersecurity Trend and Threat Analyst

EA-61 is responsible for identifying, analyzing, and cataloging relevant cybersecurity trend and threat information to support EA-62 with recommendations for inclusion into cybersecurity assessment activities. Collected trend and threat information will be correlated with priorities from the Secretary of Energy, EA, and EA-60 and may consider impact to the overall DOE mission and/or specific DOE sites.

Knowledge Management and Knowledge Development

EA-61 is responsible for KM and KD as a capability to facilitate information-gathering, sharing, and analysis in support of the overall EA-60 mission. EA-61 captures EA-62's results of classified and unclassified cybersecurity assessments throughout DOE. KM and KD efforts are specifically targeted at breaking down institutional and organizational knowledge silos, capturing institutional knowledge, and facilitating the sharing, maintaining, and updating of that data.

Assessment Support

EA-61 provides targeted support for EA-62 to inform the assessment process and provide information for potential improvements. EA-61 provides support to the assessment process in a number of key areas:

- Site Profiles and Site Profile Addendums – Site profiles are tools generated by EA-61 and are intended to inform the assessment teams during the Scoping phase of the assessment. A site profile provides a quick overview of the program to be assessed and to inform the assessment team prior to meeting with the site or program leadership. The site profile is generated 120 days in advance of an assessment and provides relevant information for

EA-62 to inform the assessment process. After the scoping meeting, a site profile addendum will be generated highlighting any data that had changed since the site profile was issued, as well as incorporating information gleaned from the site's mission brief held during scoping. Site profile addendums will be issued prior to the official start of an assessment.

- Lessons Learned – Each assessment provides a wealth of information that can be used to inform future assessments, improve the assessment process, or to capture information pertinent to the specific location. EA-61, as part of the assessment support function, gathers relevant lessons learned from post-assessment retrospectives, meetings, or other means and capture and analyzes those lessons learned for future use.
- Incorporating New Requirements into the Assessment Process – EA-61 will inform the assessment process by receiving, processing, and analyzing new Federal requirements, DOE Directives, Policies, and other official guidance. The outputs of this process will be formal recommendations for additions or other changes to portions of the assessment process to ensure the assessments remain timely, relevant, and useful for stakeholders.
- Yearly Assessment Planning – EA-61 is responsible for submitting an assessment planning report no later than June 30th of every year.