U.S. DEPARTMENT OF ENERGY

Office of Cyber Assessment Strategy

Concept of Operations

March 2020

Version 1.0

Office of Cyber Assessments

Office of Enterprise Assessments

U.S. Department of Energy

Document Version Control			
Version Number	**Change Editor**	**Date of Change**	**Description of Changes Made**
1.0	EA-61 Advisory Group	March 31, 2020	Original Document

Office of Cyber Assessment Strategy

Concept of Operations

Approval Form

Approved by: William F. West Digitally signed by William F. West Date: 2020.04.01 13:19:46 -04'00' ____________________ Date ___________

William F. West
Director
Office of Cyber Assessments (EA-60)
Office of Enterprise Assessments

Acknowledged by: Tarra D. Anthony Digitally signed by Tarra D. Anthony Date: 2020.04.01 13:13:07 -04'00' ____________________ Date ___________

Tarra D. Anthony
Director
Office of Cyber Assessment Strategy (EA-61)
Office of Cyber Assessments (EA-60)
Office of Enterprise Assessments

Table of Contents

List of Tables

1 Introduction

The Department of Energy (DOE) Independent Oversight program is implemented by the Office of Enterprise Assessments (EA). The Office of Cyber Assessment Strategy (EA-61), within the Office of Cyber Assessments (EA-60), is responsible for the strategic planning, program management, and knowledge management functions required to support EA-60's mission, as mandated in DOE Orders 227.1A Chg1, *Independent Oversight Program*, and 226.1B, *Implementation of Department of Energy Oversight Policy*. EA-60 maintains its independence by having no direct responsibility for facility operations, protection program management, information systems management, or policy formulation.

1.1 Purpose

This Concept of Operations (CONOPS) defines the functions of EA-61 to ensure EA-60 direction is aligned with the DOE mission priorities, responds to emerging threats, and that programs are managed and function efficiently.

This CONOPS is a living document. It will be reviewed and, if applicable, updated at least annually. The approved version of the guide will be available on the Energy.gov website. To ensure that this guide remains current, all users of this guide are encouraged to provide comments and recommendations to the EA-61 Director for consideration.

1.2 Scope

This guide complies with Office of Cyber Assessments CONOPS and applies to all EA-60 team members and serves as a primary resource to ensure consistency supporting strategy activities.

1.3 EA-61 Mission

EA-61 is responsible for the development of systems and procedures for tracking and monitoring cybersecurity assessments and reports, formalizing the catalog of existing cybersecurity assessment capabilities, maintaining strategic assessment requirements, and responding to specialized and ad hoc cybersecurity advisory requirements. EA-61 also analyzes cybersecurity trends and studies complex-wide issues to provide feedback on essential information assurance practices to DOE Headquarters and sites.

EA-61 functions include Knowledge Management (KM) and Program Management (PM) and is responsible for development and implementation of the required business processes and information sharing infrastructure to facilitate improved transparency, knowledge sharing, reporting, and benchmarking across the DOE Enterprise. EA-61 also executes strategic planning and information management for EA-60 and identifies internal and external capabilities required to support EA-60's mission.

2 Roles, Responsibilities, and Partnerships

2.1 Roles and Responsibilities

Each team member of EA-60 serves as an integral part of the strategy functions; however, Table 1 lists the roles and work streams (italicized) responsible for supporting the strategy functions and executing strategy deliverables.

Table 1 Roles and Responsibilities

Role / Work stream	Responsibility
EA-61 Director	• Coordinates with the EA-60 and EA-62 Director to define strategies that align with DOE mission priorities. • Oversee the execution of strategic planning, information management, and business policy development on behalf of EA-60. • Oversee the development and maintenance the information sharing capability. • Oversee Program Management Office (PMO) capability • Oversee the formalizing the catalog of existing cybersecurity assessment capabilities. • Respond to specialized and ad hoc cybersecurity advisory requirements • Maintain partnership internal and external to EA-60 to support strategy activities.
Program Management	• Executing the function of the PMO capability. • Establish process and procedures to provide for tracking and monitoring of cybersecurity assessment requirements as needed. • Establish process to provide for supporting program/project management activities execution. • Coordinate response effort to support specialized and ad hoc cybersecurity advisory suspense requirements • Maintains catalog of assessment capabilities
Knowledge Management	• Establish and maintain a process for identifying, analyzing and describing emerging threats. • Use the emerging threat information to inform the development of specific assessment strategies. • Provide historical information pertinent to each assessment lead to use as part of the initial planning and scoping process. • Provide trending information pertaining to cybersecurity assessments to the assessment leads. • Maintains information sharing capabilities.

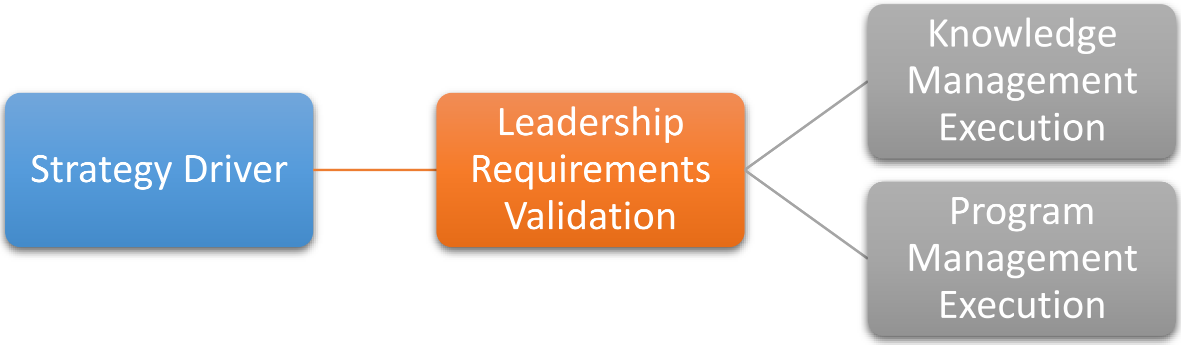
2.2 Partnerships and Collaboration

Partnerships and collaboration with external organizations and DOE entities are key components to developing strategy and analyzing emerging technology, threats, and cybersecurity trends. Outputs form our partners support the study of complex-wide issues to provide feedback on essential information assurance practices that can affect the assessment process or the direction of the organization. Below is a list of partnership that EA-61 assist in maintaining.

- DOE Cyber Council. The DOE Cyber Council is the principal forum for collaboration and coordination of cybersecurity activities across the DOE Enterprise. The members of the Council include the Deputy Secretary (Chair), Associate Deputy Secretary, CIO, and other undersecretaries, directors, and leadership of the Department. The Council's focus is on the broad sphere of cyber, including information sharing and information safeguarding. The DOE Cyber Council's responsibilities include:
    - Serving as the collaborative decision-recommending body for DOE Enterprise-wide cyber issues;
    - Exercising oversight of the Cyber Governance Framework to support effective, efficient, and secure accomplishment of the Department's mission;
    - Ensuring that the diverse array of mission perspectives is heard and, when consensus cannot be reached, document dissenting opinion(s) in relevant papers; and
    - Resolving policy conflicts elevated by lower-level bodies
- DOE Information Management Governance Board (IMGB). The IMGB ensures the DOE enterprise has efficient IT project management and oversight to support information sharing (mission enablement) and information safeguarding (mission assurance).
- DOE Insider Threat Program (ITP). ITP develops and maintains a collaborative environment to identify, coordinate, and integrate local activities to address insider threats.
- DOE Enterprise Architecture Governance Board (EAGB). The EAGB provides the governance process to decide and communicate architectural plans across the Department as well as identify the approved technology stack required to meet critical business requirements.
- Intelligence Community (IC) Inspector General (IG). The IC IG convenes intelligence communities across the Federal government to discuss and inform practices and edict impacting IC audit activities.

3 Strategy Process

Strategy drivers can originate from different sources internal and external to the EA-61 organization. EA-61 will develop assess these drivers and develop applicable protocol, process, or capability to meet addressed the immediate needs of the EA-60 organization, address requirements defined in the EA Operational Plan, Departmental, or Federal directives, or support maturing processes within EA-60. The EA-61 Director, in coordination with the EA-60 and EA-62 Directors, will define the requirements for and EA-61 work streams will execution the task for their applicable functional area.


Strategy Driver
Leadership Requirements Validation
Knowledge Management Execution
Program Management Execution

3.1 Program Management

The purpose of the Program Management work stream is to improve the transparency of the discrete processes and milestones supporting the execution and delivery of EA-60 services through the establishment of a blended supporting and controlling PMO capability. The PMO capability provides oversight of various functional areas within EA-60 to include but is not limited to: *Communications Management, Project and Schedule Management, Services Management, Change Management, Financial Management, and Compliance Management.*

3.2 Knowledge Management

The Knowledge Management work stream provides an information management capability through information-collection, sharing, and analysis to support the overall EA-60 mission of independently evaluating the effectiveness of classified and unclassified cybersecurity programs implemented throughout DOE. The KM Charter defines this process in more detail. The high-level topics discussed in this plan include:

- Development and implementation of an information sharing infrastructure. Enhancing transparency, knowledge sharing, reporting, and benchmarking, which aids in effective decision making.
- Cybersecurity trend analysis. Analyzes assessment results, emerging threats, risk information from external sources, site-specific and emerging technologies, changing Federal requirements, and other relevant information to inform the development of long-term strategies or to inform short term tactical research and development within EA-62.