U.S. DEPARTMENT OF ENERGY

Office of Cyber Assessments

Program Plan

September 2025

Version 3.0

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**
Version 1.0	Murray	12/2019	Initial release.
Version 2.0	West, Bland, McFearin, and Murray	01/2021	Update to the initial release.
Version 2.0	Cantrell and Blundin	02/2021	Technical edit
Version 2.1	McFearin	11/2021	Updates for FY22
Version 2.2	Kelly/McFearin	11/2023	Updates for FY24
Version 2.3	Unwin/McFearin	1/2024	Updates to align with key priorities
Version 2.31	McFearin	10/2024	Editorial updates and adding roles and responsibilities.
Version 3.0	McFearin	9/2025	Updating based on EA-60 restructuring

Approved by: CHRISTOPHER MCFEARIN

Digitally signed by CHRISTOPHER MCFEARIN
Date: 2025.09.29 15:31:38 -06'00'

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

Table of Contents

1. Introduction

Purpose

This program plan describes the Office of Cyber Assessments' authorities and how the office accomplishes its responsibilities. This plan outlines the mission, vision, core principles, governance, organizational structure, and capabilities that define the independent cyber assessment program operating within the Department of Energy (DOE) Office of Enterprise Assessments (EA).

Authorities

The DOE Independent Oversight program is implemented by 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 the Office of Cyber Assessments (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 (NNSA) national security and intelligence systems to meet the annual independent requirements of the Federal Information Security Modernization Act (FISMA) of 2014.

DOE Order 205.1, *Department of Energy Cybersecurity 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. DOE Order 205.1 also defines requirements for developing and reporting on corrective actions (i.e., plans of action and milestones) related to weaknesses identified during EA cyber assessment activities.

Implementation

Using these authorities, EA-60 implements the Department's independent oversight cybersecurity assessment program in accordance with applicable requirements and approved internal protocols. EA-60 is responsible for evaluating, assessing, and reporting on the effectiveness of the DOE cybersecurity programs, including those of the NNSA and contractor organizations, Office of Environmental Management, Office of Science, Power Marketing Administrations, Office of Intelligence and Counterintelligence, and all other Departmental Elements under DOE. EA-60 also develops the annual FISMA assessment metrics and reports for DOE national security and intelligence systems. EA-60 conducts extensive planning to tailor assessment activities appropriately. This aids in characterizing assessment results in the most meaningful way to further the mission of the Department. Additionally, EA-60 conducts special assessments as requested by the Office of the Secretary or other stakeholders, performs follow-

up actions for concerns identified during assessment activities as required, and shares a summary of results, lessons learned, common issues, and good practices derived from the assessments performed across the Department. EA-60 also collaborates with numerous entities within and outside EA to remain aware and knowledgeable of the Department's priorities and challenges throughout the Federal government.

2. Mission and Vision

EA-60's Mission

EA-60 conducts independent evaluations of the effectiveness of classified and unclassified cybersecurity programs throughout the Department. EA-60 uses its knowledge and expertise of the DOE missions to develop threat-informed assessment programs that provide results to risk decision makers to enhance their cybersecurity capabilities and support the secure enablement of the site and program missions. These activities include tailored cybersecurity program performance assessments in critical areas needed to protect the information, systems, and technology assets from cyber threats. In addition, EA-60 uses technical performance testing to evaluate security defenses and incident response capabilities. The EA-60 assessment teams may also exploit vulnerabilities to demonstrate the potential impact if leveraged by an adversary or malicious insider. These activities are aligned with the risk management framework and oversight requirements outlined by national policy and DOE Orders.

EA-60's Vision

To be the premier cybersecurity assessment organization for the Department of Energy by supporting our stakeholders with valuable information to assist in making effective risk decisions.

Core Principles

Our culture is a key component of our organization's ability to achieve our mission. Culture provides the intangible factors that enable our team to provide the highest quality assessment services while supporting our most important asset: our people.

The core principles enabling this culture include our values, our expertise, and our continuous learning. These principles provide a framework for how our offices work with each other and with our stakeholders and describe the characteristics of our team both individually and collectively. Enhancing the workplace culture is a priority for EA-60 to promote an environment that motivates and empowers the team, leverages expertise, and encourages continuous improvement.

These principles and the supporting performance characteristics are depicted below.

Values

- Respect others and be curious.
- Support each other and our stakeholders.
- Praise good behavior; call out negative behavior.
- Be personally accountable for your work.
- Promote trust through open and transparent communication.

Expertise

- Develop tools and techniques to address the Department's top priorities and threats.
- Analyze and correlate assessment results into impactful information for use by risk decision makers.
- Give our people the right tools to do their best.

Learning

- Strive for excellence, not compliance.
- Build enduring solutions.
- Start simple, iterate, learn, and improve.

Culture is foundational to supporting our mission. The mission requires specific actions to execute the EA-60 vision. However, those actions require enabling leadership and direction to incorporate our cultural principles with our mission. These core principles will be used as a model for leadership and workplace culture in the office and will guide our decisions and priorities to achieve the EA-60 mission.

3. Governance and Organizational Functions

With support from other Federal management and contractor resources, the EA-60 Director leads the development and prioritization of initiatives and overall program management. The EA-60 Director is the Senior Federal Executive responsible for management of all EA-60 assessment policy, planning, and operations of this office. The Director forecasts the budget and costs for travel, training, and other direct costs and serves as the conduit for all external communications. The Director is also responsible for developing and maintaining the EA-60 workplace culture, ensuring respect, accountability, continuous learning, and delivery of high-quality results to EA-60's stakeholders. The Director is also responsible for ensuring that all Federal and contractor EA-60 employees adhere to DOE and site-specific safety and security program requirements when conducting assessment activities at DOE sites. The Director is the rating official for the Federal staff and serves as a technical monitor for the support services contract.

The Director communicates objectives for projects, priorities, and assessment activities to the EA staff and stakeholders through informal and formal methods (e.g., emails, memorandums, reports, policies, performance plans, contract performance feedback) and during structured

meetings (e.g., leadership and staff meetings, post-assessment briefings).

Threat-Informed Assessments Planning, Conducting, and Reporting

EA-60 is responsible for conducting in-depth threat analysis, high-level focused evaluations, and effective knowledge management practices. With a primary focus on emerging cybersecurity information, regulatory requirements, and stakeholder input, the team strives to enhance the overall effectiveness of cybersecurity assessments by providing decision support to EA leadership, enhancing threat information to assessment leadership, and ensuring efficient knowledge utilization within the organization. Additionally, EA-60 develops threat information and site reference information and correlates relevant cybersecurity incidents, site cybersecurity conditions, emerging cybersecurity requirements, and other relevant information to enable a more effective review of cybersecurity programs across the Department.

Using this threat information and its subject matter expertise of DOE, EA-60 is better informed to complete its initiating, planning, conducting, and reporting responsibilities for cybersecurity assessments. The goal of these assessments is to evaluate the effectiveness of classified and unclassified cybersecurity programs implemented throughout the Department. The office has established and maintains a continuous program for assessing the security of DOE sites and cybersecurity programs through remote and onsite program reviews, using a variety of assessment techniques (e.g., interviews, technical analysis) performed by Federal and support services contractor subject matter experts (SMEs).

EA-60 uses its historical knowledge of DOE to enhance information is gathered as part of ongoing collaboration with DOE and during assessment planning to better understand each assessed cyber program and technical implementation to plan and scope the assessment appropriately. EA-60 combines this information with interviews and technical performance testing to evaluate a program's ability to effectively manage risk, detect and respond to malicious activity, and detect weaknesses that can be exploited by adversaries. As part of these activities, EA-60 develops and delivers a series of assessment reports each year that document the analysis and results of each cybersecurity assessment. The Federal staff and support services contractor also analyze, summarize, and combine these results into briefings and other artifacts to support sharing results throughout the Department.

EA-60 capabilities include replicating the techniques, tactics, and practices of adversaries and serving as SMEs for cybersecurity in project teams and other forums where they represent EA. The SMEs support EA-60 with independent studies of cybersecurity topics of interest to the DOE community and perform reviews of cybersecurity topical areas that support the analyses to identify crosscutting and emerging issues.

Additional information related to the assessment process itself, including roles and responsibilities, can be found in the Office of Cyber Assessments – Assessment Process Guide (external link).

4. Assessment Capabilities, Methods, and Results

Cyber threats are continuously increasing across the Department and the Federal Enterprise, and adversaries continue to enhance their techniques, tactics, and practices. Resources, both personnel and technology, also continue to be a challenge across DOE. EA-60 must continue to evolve its processes and results to support informed risk decisions and resource allocation by DOE leadership. Therefore, it is a priority for EA-60 to ensure ongoing development and implementation of technologies and processes to maintain advanced, threat-informed programs and technical assessment capabilities. These capabilities then provide results used by DOE to enhance its cybersecurity programs. The following is a list of examples of these capabilities and results provided through the EA-60 assessments.

Assessments and Special Project Capabilities

- Conduct approximately 15–18 (announced and unannounced) assessments annually
- Assess sensitive compartmented information facilities, special access programs, industrial control systems, software applications, physical access control systems, High Value Assets (HVAs), national security systems, and intelligence systems
- Develop threat reports and other knowledge management artifacts to define and support assessment strategies
- Conduct special projects: e.g. continuous network scanning

Assessment Methods

- Programmatic Review
  - Local implementation and requirements analysis
  - Cyber oversight and governance review
  - Issues management effectiveness review
  - Correlation of technical implementation weaknesses to process failures and/or process weaknesses to technical vulnerabilities
- Technical Testing
  - Testing effectiveness of security and defense-in-depth measures
  - Using insider-focused tactics and threat-informed methods
  - Evaluating incident response capabilities and performance
  - Determining detection effectiveness
- Results Analysis
  - Issues and strengths in the context of the mission
  - Impact of weaknesses based on defense in depth
  - Effectiveness of issues management processes to prevent recurrence
  - Ability for oversight to effectively monitor performance

Assessment Results

- Learning and Collaboration

  - Gathering retrospectives and lessons learned to inform future assessments
  - Gathering report and assessment feedback from leadership to inform future assessments
  - Developing good practices and cross-cutting issues for briefing senior leadership and sharing with the DOE cyber community
  - Collaborating with other EA offices to identify cross-cutting issues
- Reports, White Papers, and Briefings
  - Annually produce ~20 reports, including the DOE's Intelligence Community Inspector General FISMA report and DOE National Security Systems FISMA metrics
  - Brief the Departmental Elements, Energy Facility Contractors Group, working groups, and others on the latest results and observations from assessments and ongoing evaluations

5. Stakeholders and Collaboration

Effective execution of the mission requires collaboration with stakeholders internal and external to DOE. The following table outlines the stakeholders with which EA-60 partners to accomplish its mission.

Stakeholders	Role
Departmental Leadership	- Provide strategic vision and prioritization of key initiatives that impact the organization - Provide feedback on assessment approach - Provide priorities and focus areas for assessments
EA Leadership	- Propagate policy oversight of independent assessments - Provide strategic vision and prioritization of key initiatives that impact the organization
Departmental Elements	- Leverage EA assessment services - Provide mission/business input and expertise to assist in EA planning
Other EA Offices	- Provide additional enforcement, assessment, and training information to aid in planning and conducting cyber assessments - Collaborate on combined assessment activities - Share lessons learned, results, and cross-cutting issues

Stakeholders	Role
DOE Office of the Chief Information Officer	- Provide enterprise risk analysis and information technology program support - Lead and cultivate the Privacy Program for the Department - Create and disseminate cyber training and awareness - Partner with the Departmental Elements to assess and report on the HVAs and completion of corrective actions - Provide supply chain risk management evaluations - Provide incident awareness and reports from the enterprise - Provide key site and enterprise information from incident reports, network tools, data calls, and other sources to support the EA mission - Provide information technology resources and collaboration tools to facilitate communication and information exchange to support the EA mission
NNSA Office of the Chief Information Officer	- Provide incident awareness and reports from the NNSA enterprise and classified networks - Provide results from enterprise cybersecurity exercises for collaboration with the EA mission - Collaborate with EA on assessments of high-priority projects
DOE Office of the Inspector General	- Coordinate annual assessments, prioritization, and deconfliction between Inspector General audit and EA assessment activities - Coordinate with EA on annual FISMA metrics for DOE information systems - Address special projects related to DOE Office of Intelligence and Counterintelligence information systems
Department of Homeland Security	- Engage with DOE regarding the HVA program - Utilize EA assessment results for inclusion in the DOE HVA program
Intelligence Community Inspector General	- Provide annual intelligence community FISMA metrics - Provide input and expertise to support the EA mission
NNSA-Information Management Inspection Team	- Coordinate annual assessments, prioritization, and deconfliction
Office of Environmental Management Mission Information Protection Program	- Coordinate annual assessments, prioritization, and deconfliction
Office of Cybersecurity, Energy Security, and Emergency Response	- Coordinate sharing of key threat or risk information for critical infrastructure within DOE - Collaborate on consequence-driven, cyber-informed engineering assessment capabilities

Collaboration

EA-60 works with the stakeholders above to share our results, deconflict priorities, and ensure alignment with mission-related activities. Stakeholder engagement allows EA-60 to build strategies and threat information and to plan and conduct assessments that provide results that positively impact and enable the mission of DOE. EA-60 shares assessment results through a variety of work and ongoing interactions, including:

- Participating in other EA offices' report reviews to provide insight and comments.
- Collaborating with the Office of the Chief Information Officer and counterpart organizations across the DOE Enterprise in working groups for policy development, implementation of the latest requirements, and new initiatives to improve cybersecurity.
- Participating in DOE-sponsored boards and groups, such as the:
  - Cyber Information Technology/Operational Technology Executive Council,
  - HVA Program Management Office,
  - Information Management Governance Board,
  - Enterprise Architecture Governance Board,
  - Chief Information Security Officer Roundtable, and
  - Insider Threat Working Group.
- Conducting stakeholder engagements to better understand the unique mission aspects and risks across DOE sites.
- Conducting strategic engagements with Departmental Elements, the Energy Facilities Contractor Operations Group, and the National Laboratories Chief Information Officers council to gain insights into their priorities as well as gather feedback on our assessment results, and share lessons learned.
- Developing and leading EA Learning Sessions to discuss EA-60 results, crosscutting issues, and cyber happenings with the larger EA office.
- Presenting at Departmental Element briefings, contractor working groups, and other project teams on EA-60 cyber assessment results, common issues, and good practices.
- Developing roll-up reports of key issues within the Departmental Elements and briefing those on a routine basis to senior management.

The office will continue to expand its collaboration and engagement by providing subject matter expertise for review and comment on congressional bills, Departmental cybersecurity policy, and other documents as requested.

6. Learning and Improving

EA-60 gathers lessons learned and other retrospective data points to help identify what processes work well and where changes might be needed. Over multiple assessments and activities, EA-60 analyzes this data for relevance and applicability. The output of this process is improvement initiatives that will be prioritized for implementation. The Director may also identify specific

initiatives based on the needs and priorities of the Department.

The EA-60 Federal staff and the support services contract management work to develop objectives for improvement initiatives and then assign resources to participate in the development of potential solutions. The overall process is agile and iterative to build the best, enduring solutions. The assessment process and cybersecurity in general are not linear and require this flexibility to avoid static checklist/compliance-based processes, which will not meet the growing needs of our stakeholders.

All these efforts support enhancing the performance-based evaluation of cybersecurity programs and delivery of valuable results for the Department.

7. Non-Assessment Activities: Leveraging Expertise to Enable the DOE Mission

While many of the EA-60 staff are primarily engaged in conducting cybersecurity assessments, their expertise and knowledge are valuable assets that can be leveraged between assessments to drive continuous improvement and support the broader DOE mission. This section outlines the responsibilities and activities of EA-60 staff when not directly involved in assessments, emphasizing knowledge sharing, addressing key office priorities, threat analysis, program enhancement, and strategic engagement, particularly as it relates to summarizing and sharing assessment results with senior leadership and fostering collaboration with other DOE programs.

EA-60 Director:

- **Strategic Vision:** The Director continues to monitor the overall DOE cybersecurity landscape, identifying emerging threats, trends, and policy developments that could impact the assessment process and the secure enablement of the DOE mission.
- **Resource Allocation:** The Director ensures that EA-60 resources are allocated effectively to support ongoing training, professional development, and the development of new assessment tools and techniques that enhance the security posture of DOE's critical systems and programs. This includes resource allocation for both federal and contractor staff and the overall budget management for EA-60.
- **Collaboration and Sharing:** The Director remains actively engaged with other DOE offices, stakeholders, and external organizations to foster collaboration, share best practices, and gather valuable insights. The Director also leads the effort to share key findings from assessments with DOE senior leadership, including the Secretary, Deputy Secretary, and other senior officials, ensuring that the insights gleaned from assessments are effectively communicated and used to inform decision-making. This includes working closely with the DOE OCIO to gather information on Departmental priorities and participate in key initiatives that inform EA-60's assessment strategy and align with DOE mission objectives.
- **Stakeholder Engagement:** The Director engages with stakeholders to gather feedback on the assessment program, address concerns, and ensure that EA-60's activities are

aligned with DOE's priorities and mission objectives. This includes presenting and discussing key findings from assessment reports with DOE leadership and program offices, highlighting the impact on mission-critical systems and operations.

- **Program Enhancement:** The Director champions initiatives to enhance the effectiveness of the assessment program, such as developing new assessment methodologies, refining existing procedures, and exploring the use of innovative technologies to better protect DOE's mission-critical assets that are codified in the annual operations plan for EA.
- **Technical Monitor:** The Director serves as the support service contractor technical monitor where they ensure that the contract technical direction is implemented appropriately through ongoing meetings, reports, and other artifacts demonstrating alignment with the mission and priorities of EA-60.
- **Training and Development:** The Director monitors the training and development needs for the EA-60 federal staff, ensuring that they have the necessary skills and knowledge to conduct effective assessments and communicate effectively to enhance the security of DOE's mission. This may also include overall skills and development needs for the support service contractor staff.
- **Performance Monitoring:** The Director monitors the performance of EA-60, ensuring it is effectively executing the priorities for the office, applying internal protocols, and meeting the objectives to enable the DOE mission. This includes but is not limited to the monitoring of the implementation of the annual operations plan for EA and ensuring the EA-60 priorities are being appropriately actioned and completed.

EA-60 Federal Team:

- **Knowledge Sharing:** The Federal team contributes to the knowledge management system by documenting key insights from assessments, working groups, training, or other DOE-related forums and identifying information that contributes to the development of internal guidance documents, learning sessions, or informal presentations.
- **Threat Analysis and Research:** The Federal team leverage their expertise to conduct and support research on specific threats, vulnerabilities, or attack techniques relevant to the Department, contributing their findings to the knowledge management system and future assessments.
- **Outreach:** The Federal team engage with their peers and leadership across the Department to share their expertise, raise awareness of cybersecurity threats and vulnerabilities, follow up on assessments, maintain relationships with sites and programs, and build networks of knowledge to share with others.
- **Maintaining Cybersecurity Proficiency:** The Federal team actively pursue professional development opportunities (e.g., training, participating in DOE-centric working groups) to maintain their cybersecurity expertise and keep pace with evolving threats and technologies, especially those in use at DOE.
- **Cross-Office Collaboration:** The Federal team collaborates and shares knowledge between EA-60 and other EA offices, ensuring that they are working effectively together to achieve common goals, including the sharing and analysis of assessment observations

to enhance planning as well as providing additional impact to EA-60 assessment results.

- **Program Enhancement:** The Federal team may spearhead initiatives to improve the efficiency and effectiveness of the assessment process, such as refining assessment methodologies, overseeing development of new tools, and streamlining reporting procedures to enhance the effectiveness of securing DOE's mission.
- **Strategic Support and Collaboration:** The Federal team participate in working groups and other DOE-led activities to evaluate mission priorities and contribute their expertise to the overall DOE cybersecurity program.
- **Projects:** The Federal team will lead and/or participate in the development and delivery of key milestones for EA-60 that are documented in the annual EA operational plan. These initiatives may support a variety of improvement projects, knowledge sharing, collaboration, or team building activities where the Federal team's expertise is used to deliver successful results on time. The Federal team may also lead special projects of their own choosing if they align with the direction of the EA-60 Director.

Contractor Team Members:

- **Skill Development:** All team members are encouraged to pursue professional development opportunities, enhancing their cybersecurity expertise through training and/or participation in industry conferences, focusing on skills and knowledge that directly support assessments of DOE cybersecurity and the technologies in use throughout the Department.
- **Knowledge Sharing:** Team members contribute to the knowledge management system by documenting their experiences, sharing insights, and providing feedback on assessment tools and techniques, with a focus on how they can be used to enhance mission security.
- **Community Engagement:** Team members participate in relevant industry groups, forums, and conferences to stay current on cybersecurity trends, emerging threats, and best practices, sharing their knowledge and findings with the broader DOE cybersecurity community, with a focus on how to protect the DOE mission.
- **Report Development:** Individual team members, based on their specific expertise, contribute to the development of roll-up reports, providing analysis and insights on specific threats, vulnerabilities, and areas for improvement, with a focus on the impact on mission-critical systems and operations.
- **Project Support:** The team will support the Federal staff in the delivery of key milestones for EA-60 that are documented in the annual EA operational plan. The team may also support the Federal team on special projects at the direction of the EA-60 Director.
- **Technical Editing:** Technical Editors review and edit documents developed by EA-60, ensuring clarity, accuracy, and consistency.
- **Administrative Support:** Administrative Assistant support managing the review tasks, office updates, EA data call responses, and all correspondence traffic for EA-60; they are also responsible for coordination of assessment results briefings, dissemination of report

artifacts, and scheduling of resources to support Department meetings and events.

By actively leveraging their expertise and engaging in continuous improvement, EA-60 staff play a critical role in strengthening DOE's cybersecurity posture, even when not directly involved in assessments. This focus on delivering our operational plan items, knowledge sharing, threat analysis, program enhancement, strategic engagement, effective communication of assessment results, and collaboration with key DOE offices ensures that EA-60 remains a valuable resource for the Department and effectively supports its cybersecurity mission, ultimately securing the DOE's critical operations and programs.