U.S. DEPARTMENT OF
ENERGY

# Office of Cyber Assessments

# Concept of Operations

**November 2021**

**Version 2.1**

**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 | 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 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Office of Cyber Assessments**
**Concept of Operations**
**Approval Form**

Approved by:

CHRISTOPHER MCFEARIN

Digitally signed by CHRISTOPHER MCFEARIN
Date: 2021.11.30 04:57:18 -07'00'

Christopher E. McFearin
Acting Director/Deputy Director
Office of Cyber Assessments
Office of Enterprise Assessments

Acknowledged by:

Joseph Lewis, Sr.

Digitally signed by Joseph Lewis, Sr.
Date: 2021.11.29 08:52:21 -06'00'

Joseph Lewis
Director
Office of Cyber Assessment Strategy
Office of Enterprise Assessments

TIMOTHY SCHWAB

Digitally signed by TIMOTHY SCHWAB
Date: 2021.11.29 16:03:26 -05'00'

Timothy B. Schwab
Director
Office of Cyber Assessment Operations
Office of Enterprise Assessments

**Table of Contents**

1. Introduction ..... 4
Purpose ..... 4
Authorities and Governance ..... 4
Mission ..... 4
2. Organizational Overview ..... 5
Office of Cyber Assessments (EA-60) ..... 5
Office of Cyber Assessment Strategy (EA-61) ..... 6
Office of Cyber Assessment Operations (EA-62) ..... 7
3. FY 2022 Strategic Goals and Objectives ..... 7
4. Stakeholders ..... 8
Assumptions ..... 9
Risks ..... 10
5. Appendix A: Fiscal Year 2021 Key Accomplishments ..... 11
6. Appendix B: Legislation, Federal Directives, and Mandates ..... 19

# 1. Introduction

## Purpose

This concept of operations (CONOPS) document describes the mission, organizational structure, and services provided to support the independent cyber assessment activities of the Office of Cyber Assessments (EA-60) operating within the Department of Energy (DOE) Office of Enterprise Assessments (EA). EA-60 is responsible for evaluating, assessing, and reporting on the DOE cybersecurity programs, including those of the National Nuclear Security Administration (NNSA) and contractor organizations.

## Authorities and Governance

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 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 NNSA national security and intelligence systems to meet the annual independent evaluation requirements of the Federal Information Security Modernization Act (FISMA) 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 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 fiscal year (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 is responsible for conducting independent assessments of safety and security policies, programs, and operations throughout DOE; implementing congressionally authorized enforcement functions in the areas of worker safety and health, nuclear safety, and classified information security; and developing and providing safety- and security-related training promoting the proficiency and competency of the DOE workforce.

EA-60 conducts independent evaluations of the effectiveness of classified and unclassified

cybersecurity policies and programs throughout the Department, which includes conducting extensive network penetration testing to detect vulnerabilities and identify risks that could be exploited by adversaries or malicious insiders.

EA-60 implements the Department's cybersecurity independent oversight assessment program in accordance with applicable requirements and approved internal protocols and develops the annual FISMA assessment reports for DOE national security and intelligence systems. 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 best practices from oversight activities across the Department.

## 2. Organizational Overview

### Office of Cyber Assessments (EA-60)

As cyber risks have increased across the Department, and as the techniques, tactics, and practices of adversaries continue to evolve, EA-60 must ensure that it can efficiently assess the cybersecurity programs within identified cyber function areas. Development and implementation of technologies and processes to maintain advanced, risk-informed programs and technical assessment capabilities support the critical missions of the Department. In support of this mission, EA-60 is divided into two sub-offices: Office of Cyber Assessment Strategy (EA-61) and Office of Cyber Assessment Operations (EA-62).

Figure 1 depicts the EA-60 organization.

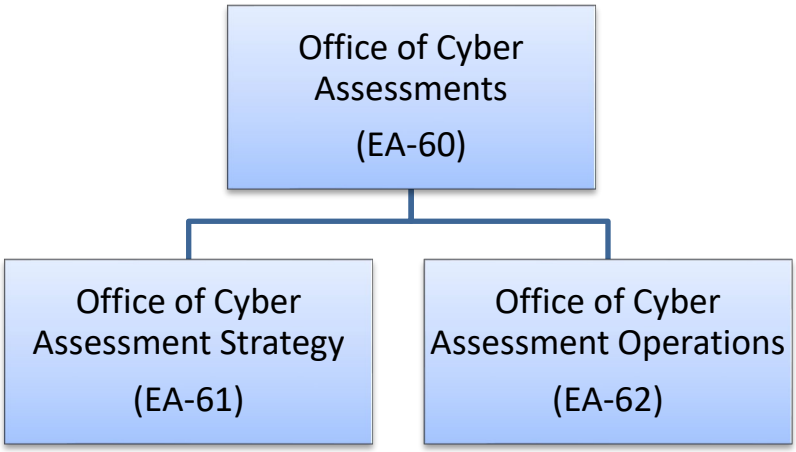


**Figure 1: EA-60 Organization Chart**

The Office of Cyber Assessments is responsible for performing independent evaluations of the effectiveness of classified and unclassified cybersecurity policies and programs throughout the Department. The EA-60 Director leads the development and execution of priorities along with

the EA-60 Deputy Director, with support from other Federal management and contractor program resources, as outlined in the current Office of EA fiscal year operational plan.

EA-60 collaborates with Department cyber and information technology governance bodies, including participation on the DOE Cyber Council, the DOE Information Management Governance Board, and the DOE Enterprise Architecture Governance Board. EA-60 participates in the DOE Insider Threat Working Group and the quarterly DOE Intelligence Community Office of the Inspector General meetings and is a representative on the Chief Information Security Officer (CISO) Roundtable.

EA-60 supports the development, coordination, and reporting of projects across EA-60. The Office is responsible for the development of systems and procedures for logistics support, and the tracking and monitoring of cyber assessments and reports. The Office is also responsible for maintaining the catalog of existing cyber assessment capabilities and supporting the development of new assessment practices. EA-60 implements policies and procedures to effectively respond to reviews of significant issues relating to protection of DOE information systems and emergent cyber assessment needs of the Department.

The EA-60 Director is the Senior Federal Executive responsible for all assessment policy, planning, and operations of this office. The Director forecasts the budget and expenditures for travel, training, and other direct costs and serves as the conduit for all external communications. The Director is responsible for ensuring that EA-60 employees adhere to site-specific safety and security program requirements when conducting assessment activities at DOE sites. The Director is the rating official for the EA-60 Deputy Director and serves as a technical monitor for the support services contract.

The EA-60 Director is supported by the Deputy Director, Office of Cyber Assessments. The Deputy Director acts on behalf of the Director in managing all functions of the Office and is responsible for all Operations and Strategic Assessments functions within EA-60. The Deputy Director is the rating official for the Directors of EA-61 and EA-62.

The Director and Deputy Director communicate all activities (e.g., status on all assessments, projects, and initiatives) 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, staff, post-assessment briefings).

## Office of Cyber Assessment Strategy (EA-61)

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 knowledge development and management 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.

### Office of Cyber Assessment Operations (EA-62)

The Office of Cyber Assessment Operations is responsible for the independent evaluation of 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 classified and unclassified networks through expert program and technical analysis, including detailed network penetration testing to detect weaknesses that could be exploited by adversaries.

EA-62 is responsible for the development, planning, and execution of all technical and programmatic cybersecurity assessment services that EA is tasked to conduct. As part of these services, EA-62 develops and delivers a series of assessment reports each year documenting the analysis and results of the cybersecurity assessment engagements. EA-62 is composed of the Programmatic and Technology assessment functions. EA-62 conducts the annual evaluation of DOE classified and intelligence cybersecurity programs and develops the associated reports, as required by FISMA.

EA-62 capabilities include replicating the techniques, tactics, and practices of adversaries and serving as a center of excellence for cybersecurity technology. Additionally, EA-62 supports EA-60 with independent studies of cybersecurity topics of interest to the DOE community and performs reviews of cybersecurity topical areas and analyses to identify trends and emerging issues. A core function of EA-62 is to develop and maintain a cybersecurity testing platform to evaluate the effectiveness of state-of-the-art cybersecurity processes and technologies implemented across the DOE Enterprise. EA-62 is led by the Director, Office of Cyber Assessment Operations, with support from EA-60 Federal and support services contractor staff.

## 3. FY 2022 Strategic Goals and Objectives

Cybersecurity is critical to the success of the Department's varied missions: maintaining the nation's nuclear deterrent, reducing the threat of nuclear proliferation, overseeing the nation's energy supply, and managing the science and technology powerhouse of the 17 National Laboratories. Protecting these vital missions from ever-growing and complex cyber threats is crucial. EA-60 complements the Department's protection through the following EA Strategic Goals (SG) articulated in the EA *Fiscal Year 2022 Operational Plan, October 2021*.

**SG1: Conduct value-added independent oversight activities that strengthen the safety and security of workers and the public, the environment, and the Department of Energy's physical, cyber, and information security assets.**

**SG4: Enhance the use of risk-informed and fact-based analysis to identify and communicate emerging trends in safety, security, and cybersecurity within the Department of Energy.**

**SG6: Expand collaboration across EA's spheres of expertise and stakeholders.**

These three strategic goals are enabled by the following seven objectives:

1. Evaluate the effectiveness of classified and unclassified cybersecurity policies and protections throughout the Department using threat-informed, expert program and technical analysis.
2. Maintain and enhance strategic cybersecurity assessment requirements and processes, and respond to specialized, ad hoc, or new cybersecurity requirements.
3. Report annually on the maturity of the implementation of cybersecurity protections for DOE national security systems and intelligence systems.
4. Analyze cybersecurity trends, threats, requirements, and Department-wide issues to inform our assessment process and provide feedback to our stakeholders on essential information assurance practices.
5. Provide programmatic and technical cyber expertise to other DOE and EA offices.
6. Provide analysis of cybersecurity assessment results to other offices to support ongoing data analytics.
7. Collaborate with other EA offices on assessment activities and unified messaging for reports.

The actions required to meet these objectives are established in the EA *Fiscal Year 2022 Operational Plan, October 2021*, and are tracked in EAShare. Those actions are promulgated to each Federal employee via the performance plan process and to the support services contractors via the technical direction memorandum.

## 4. Stakeholders

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.

**Table 1: EA-60 Mission Partners**

| Stakeholders | Role |
|---|---|
| Departmental Leadership | - Provide strategic vision and prioritization of key initiatives that impact the organization |

| Stakeholders | Role |
|---|---|
| | - Report cyber risks/trends analysis |
| EA Leadership | - Propagate policy oversight of independent assessments<br>- Provide strategic vision and prioritization of key initiatives that impact the organization |
| Departmental Elements | - Leverage EA assessment services<br>- Provide mission/business input and expertise to support the EA mission |
| DOE Office of the Chief Information Officer | - Provide enterprise risk analysis and IT program support<br>- Lead and cultivate the Privacy Program for the Department<br>- Create and disseminate cyber training and awareness<br>- Partner with the Departmental Elements to lead and report on the High Value Asset program<br>- Sponsor and host the incident response leaders' forum to bring together key cyber defenders to discuss challenges and trends<br>- Provide supply chain risk management evaluations<br>- Provide incident awareness and reports from the enterprise<br>- Provide key site information from data calls and other sources to support the EA mission<br>- Provide information technology resources and collaboration tools to facilitate communication and information exchange to support the EA mission |
| DOE Office of the Inspector General | - Coordinate annual assessments, prioritization, and deconfliction<br>- Provide annual FISMA metrics for DOE information systems |
| Department of Homeland Security | - Engage with DOE regarding the High Value Asset program<br>- Evaluate EA assessment results for inclusion in the DOE High Value Asset program |
| Intelligence Community Inspector General | - Provide annual intelligence community FISMA metrics<br>- Provide input and expertise to support the EA mission |
| NNSA-Information Management Inspection Team | - Coordinate annual assessments, prioritization, and deconfliction |

## Assumptions

Key assumptions driving the success of the 2022 EA-60 CONOPS are as follows:

- EA mission does not change.
- EA-60 Federal staffing levels (as defined by the EA staffing plan) will not change in FY 2022.
- EA-60 contractor staffing levels (as defined in the contract) will not change in FY 2022.
- EA-60 funding levels will be consistent with the budget requested for FY 2022.

- FISMA reporting requirements will not change in FY 2022.

## Risks

Risks that could impact EA-60's ability to complete the goals, objectives, and actions outlined in the EA Operational Plan are listed below with the associated mitigations.

**Table 2: Risks and Mitigations**

| Risks | Mitigations |
|---|---|
| COVID-19 Effects | - Adapt existing processes to support remote and hybrid programmatic and technical assessment requirements.<br>- Focus assessment scope. |
| Mission Change | - Develop new or adapt existing processes to address mission expansion or mission focus requirements. |
| Budgetary Constraints | - Reduce scope or quantity of assessments prioritized by risk or threats to Department mission. |
| Staff Turnover | - Continue development of Federal staff to ensure minimal impact through succession planning.<br>- Continue development of the contractor staff by continuing to build leadership experience within the team and defining an initial succession plan for key contractor staff position |
| Continuing Resolution | - Work with EA financial team to ensure funding levels are sufficient to continue work. Provide detailed analysis of the duration that work may continue and streamline activities accordingly. |

## 5. Appendix A: Fiscal Year 2021 Key Accomplishments

During fiscal year (FY) 2021 (defined as September 2020 through August 2021), the Office of Cyber Assessments (EA-60) updated and realigned the mission of the Office of Cyber Assessment Strategy (EA-61) to focus on the development and integration of threat information into the Office of Cyber Assessment Operations (EA-62) processes, and on knowledge management for EA-60. These updates better align the Offices to one another and provide more flexibility to meet the priorities and mission requirements of the Department and the Office of Enterprise Assessments (EA) leadership. The Coronavirus Disease 2019 (COVID-19) pandemic and the resulting maximum telework throughout the Department of Energy (DOE) required EA-60 to pivot its capabilities and perform assessments remotely and/or with only a limited onsite presence. EA-60 conducted 18 announced remote and hybrid cyber assessments (EA-60-2021-001 and EA-60-2021-005) as scheduled. Of these assessments, three were requests made during the year from the DOE Office of the Chief Information Officer (OCIO), Office of Environmental Management, as well as the National Nuclear Security Administration to assist in assessment of potential threats to not only DOE but also to national security. Included in the assessment activities this year, EA-60 completed two high value asset (HVA) assessments for the Department to help meet DOE's Agency Priority Goal for FY21. Late in 2020, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency recognized EA-60's assessment of Bonneville Power Administration from January 2020 as fulfilling the requirement for a Tier 1 HVA assessment. This is significant, as most Tier 1 HVA assessments must be conducted by DHS. This recognition reduced the assessment burden for the Department (EA-60-2021-004). Notably, EA-60 was able to keep a high operations tempo during the COVID-19 pandemic while prioritizing safety for EA and site personnel and expanded its remote and hybrid assessment capabilities.

EA-60 also filled critical vacancies, including EA-60 Deputy Director, EA-62 Director, and two staff positions within EA-62. The EA-61 Director has been selected, and we are awaiting a start date. The hiring process is moving forward for the remaining staff positions. The onboarding process was unique during the pandemic, but the team met the challenge to indoctrinate the new hires, worked together to teach and mentor, and established a team dynamic and culture despite the remote work.

<u>Outreach & Collaboration Activities</u>

**Outreach**

- Spearheaded the 2021 Feds Feed Families initiatives for EA.
- Participated in the following conferences: Black Hat, DEF CON, CactusCon, and National Laboratories Information Technology Summit.
- Participated in the quarterly Intelligence Community Office of the Inspector General (IG) meetings.

- Briefed the EA Office regarding EA-60's response to the COVID-19 pandemic, including lessons learned from the development and refinement of remote and hybrid assessments (EA-60-2021-013).
- Completed an EA-60 Federal Workshop, a group of four sessions throughout FY21 that focused on leadership and strategy for EA-60; EA-60's integration with other EA offices in support of further collaboration; strategy and planning for FY22, including a focus on EA-1's priorities (may also be used for operational plan development); and leading change within EA-60 and ensuring we are meeting the Department's priorities (EA-60-2021-018).
- Conducted a programmatic workshop focusing on National Institute of Standards and Technology (NIST) 800-53 Revision (Rev) 5, differences from NIST 800-53 Rev 4, potential impacts to EA-60 assessments, and how NIST 800-53 Rev 5 will impact EA-owned systems (EA-60-2021-018).
- Co-developed and facilitated three Authorizing Official (AO) training courses in coordination with the DOE OCIO AO Training Team.
- Co-developed and facilitated one system owner training course in coordination with the DOE OCIO Training Team.
- Participated in the monthly CISO roundtable; Local Insider Threat working group; High Value Asset Stakeholder group; DOE Supply Chain Risk Management group; Control Systems Working Group; the DOE Phishbowl (i.e., phishing awareness group); and the DOE Identity, Credential, and Access Management working group.
- Participated in the monthly Safeguards and Security collaboration meetings.
- Collaborated with the DOE OCIO to integrate their information provided by the integrated Joint Cybersecurity Coordination Center (iJC3) and crowd-sourced assessment capabilities into the assessment planning process (EA-60-2021-011).
- Collaborated with other EA Offices on the review of the EA Mission, Vision, and Value statements and provided meaningful feedback and updates for the FY22 Operational Plan.
- Continued to collaborate with Office of Safeguards and Security Assessments (EA-20) on unified assessments for secure facilities and ensuring that reporting is consistent across both offices. Due to COVID-19, assessments had been rescheduled or postponed and did not provide the opportunity to perform combined assessments. A POAM will be added to the FY22 Operational Plan, and coordination is already underway with EA-20 (EA-60-2021-019).
- Completed the National Security System and Intelligence Community Federal Information Security Modernization Act (FISMA) reports (EA-60-2021-008 and EA-60-2021-009).
- Provided cybersecurity subject matter expertise for the Office of Environment, Safety, and Health Assessments (EA-30) led independent software quality assurance (SQA) oversight analysis working group. This group provided an analysis of current SQA requirements and practices throughout the Department and developed recommendations for EA leadership on additional assessment strategies as well as initial observations on the SQA policy. The group will continue to collaborate on future assessments related to SQA in 2022 (EA-60-2021-014).

- Participated in the Energy Facility Contractors Group Cybersecurity Working Group; the group was developed to promote excellence in all aspects of cybersecurity operations and management of DOE facilities through consistent exchange of information, best practices, and corresponding improvement activities.
- Collaborated with iJC3 to develop communication and relationships with the cybersecurity team to enhance EA-61's threat information by sharing the latest reports. EA-61 has established a monthly meeting with iJC3 to continue information sharing.
- Participated as a team leader for the Enterprise-wide COVID-19 pandemic lessons-learned review as well as participated in the development of the EA report for the Secretary of Energy.
- Collaborated with the Office of Security Enforcement (EA-13) to provide subject matter expertise for cybersecurity requirements related to the authorization of information systems, to determine whether processes in place were in accordance with DOE policies, and to provide background on normal processes seen at DOE locations.
- Participated as an auditor in the Western Area Power Administration's North American Electric Reliability Corporation Critical Infrastructure Protection mock audit.
- Provided cybersecurity subject matter expertise and support for FEMA's Emergency Support Function #12.
- Presented an EA Learning Session titled "Managing Cybersecurity Assessments during COVID-19 and beyond" on May 28, 2021, which discussed the processes that EA-60 developed to address remote assessments and remote work during the pandemic. The lessons learned will be applicable to post-pandemic assessments (EA-60-2021-013).
- EA-60 presented a Learning Session on cyber assessment results, trends, and operational processes on September 28, 2021 (EA-60-2021-017).
- EA-60 provided cybersecurity subject matter expertise to the National Training Center (NTC) in the form of information sharing for Emergency Directives and mitigations for NTC systems, the review of anomalous activity alerts to determine false positives, and feedback on the ongoing cyber program development project initiated by the NTC ISSM. EA-60 also partnered with the Authorizing Official within NTC for the successful deployment of EA-60's cloud system (EA-60-2021-015).

**Cybersecurity Governance:**

- Represented EA on the Information Management Governance Board, Cyber Council, Enterprise Architecture Governance Board meetings, Zero Trust/Cloud Working Group, and the DOE OCIO Incident Response Leaders Forum.
- Provided comments on several Congressional bills, Office of Management and Budget memoranda, Government Accounting Office reports, DOE IG reports, DHS Binding Operational Directives, agency leadership Congressional testimonies, and draft DOE Orders/Policies.

- Participated in the integrated project team for the development and drafting of the updated appendix to DOE Order (O) 205.1C, Vulnerability Disclosure Program.
- Participated in the integrated project team for the updating of DOE O 206.1, Privacy Program.
- Participated as a Cyber Workforce Project Team as a subject matter expert developing and defining cybersecurity competency statements for the role of DOE IT Project Manager within cybersecurity; this supported DOE Human Capital Office's goal of developing competency models for the Department.

Programmatic Process Improvements

**Improved Office of Cyber Assessments capabilities:**

- Developed a Performance-Based Risk-Informed assessment model that specifically integrates threat information and risk areas into assessments, allowing results and outcomes of assessment observations to reflect program performance. The EA-60 report format has been updated to reflect the performance-based assessment processes and results and has been incorporated for all reports for FY21. Additionally, these inputs were added to the planning and development of the specially requested NNSA Software Development Lifecycle Assessment this year, where specific risks from NNSA were used to tailor the assessment approach. The assessment provided valuable results back to leadership (EA-60-2021-007).
- Began using newly available tools Microsoft Teams and Planner for improved collaboration and coordination for projects, assessments, and sub-offices. The integration of these applications has provided improved communications among team members at no additional cost to EA-60.
- Reviewed and updated key operational processes for the planning, conducting, and reporting stages of the assessment process.
- Developed research and development processes that assign a lead and other resources to evaluate new assessment capabilities, requirements, or technology and produce artifacts that are then transitioned to the operational staff for integration into assessment operations.
- Developed assessment objectives and strategies for new requirements (e.g., DOE O 205.1C) and threats to the overall Department and the processes to integrate them into assessment operations.
- Restarted development of the lessons learned program at the initiation of the newly appointed EA-62 Director; the program focuses on continuous self-evaluation (through retrospective sessions) of the assessment process, team meetings, and other EA-60 activities to identify successes, as well as areas that can be improved.
- Created agendas and meeting minutes for weekly leadership and staff meetings.
- Created a white paper and developed a new process and a system to categorize cybersecurity threats, called Reveries, that align these threats to DOE missions. Each Reverie contains structured information allowing analysts to better focus research as well as improving data retention and searching.

- Reviewed and updated the scoping process, increasing EA-60's understanding of a site's cybersecurity program before the formal scoping call takes place.
- Developed an insider threat testing methodology standardizing programmatic and technical assessment procedures for evaluating insider threat risks across unclassified and classified systems (EA-60-2021-003).
- Conducted an IPv6 gap analysis to determine current capabilities available for testing networks using IPv6 and determine team training needs related to IPv6.
- Developed a research and development platform for testing and evaluating phishing frameworks with the goal of adding a new assessment capability to EA-60's toolkit.

**Process improvements:**

- Served as the system owner for the Cyber Assessments Mobile Platform (CAMP), the Cyber Security Testing Network (CSTN), and the Classified Facsimile and Copier Machines.
- Developed monthly system status updates to review system inventory changes, software licenses, overall system health, and any upcoming purchases.
- Developed processes to review and analyze open-source cyber threat information, integrating this information to support adversary simulation and emulation activities and to add impact to observations made during EA-60 assessments.
- Developed processes to review and analyze Departmental priorities and industry trends in cybersecurity for potential impact to DOE missions and prioritization in focus areas of cyber assessments.
- Used the security control assessor team to perform self-assessments on the CAMP and CSTN information systems along with supporting security assessment reports and results that were presented to the AO.
- Created report trackers to track reporting targets, identify potential resource conflicts, and ensure timely delivery of reports.
- Developed "point papers" for each assessment to provide initial direction from the Federal team to the lead authors.
- Maintained the CSTN instance in Germantown, including creating a hardware and software licensing tracking database, and implementing all applicable system and security updates and patches.
- Established the Information Technology (IT) Support Operations team consisting of a new Information System Security Engineering position and existing system administrator role at the Hilliard office to provide better support for CSTN maintenance and to establish a unified technology strategy for EA-60 IT resources.
- Maintained CAMP through a technical equipment refresh, upgrading old Dell laptops with new laptops from System 76.

- Established a bi-weekly sprint management plan for EA-61 task management activities. Tasks are established in a continuous backlog, discussed, and then assigned to a sprint plan to be worked during the sprint period. This has resulted in improved Federal oversight, task tracking, and documented decisions/changes.
- Developed site profiles for each assessment prior to the initial scoping meeting. These site profiles provided an overview of the site as well as the latest cybersecurity incidents, FISMA data, Enterprise Cyber Governance System data, the last cybersecurity assessment report, and any other information that was relevant to the assessment. Centralizing this information for each assessment has saved multiple work hours per assessment by eliminating the team's need to individually research this information.
- Developed an EA-60 file plan to establish processes for storing, retaining, and archiving documents.
- The EA-60 capabilities presentation outlining the EA-60 assessment process and methodology has been fully updated and put on a regular schedule for updates to ensure it remains current and available when required (EA-60-2021-010).
- The scoping procedures for EA-60 have been updated to include site, threat, and additional information from leadership as part of the planning processes. This work has been augmented by threat information research and processes implemented by EA-61 (EA-60-2021-011).
- EA-61 has created a briefing template that, when populated, will display assessment results and report information from previous assessments and can provide additional cyber trend or other cyber-related information. This template will be updated based on the needs of our stakeholders while ensuring uniformity with other EA offices (EA-60-2021-016).

**Improved and expanded tools:**

- Continued to expand the capabilities of the knowledge management system that provides information from our cyber assessments conducted in DOE from 2012 to present. This system provides dashboard statistics related to findings, deficiencies, opportunities for improvement, and best practices correlated with cybersecurity requirements to DOE and EA leadership.
- Developed "SPECTRE," an enhancement to the existing "day one" scanning and enumeration script via the research and development workstream, improving EA-60's ability to quickly enumerate site networks.
- Continued to expand and refine the capabilities of the Continuous Network Scanning system and moved deployment from collocated data centers to a cloud hosting environment. The team is actively using the new capability and providing results back to our assessment teams (EA-60-2021-006).
- Improved the deployment capabilities of the Remote Assessment Penetration Testing Operations Resource (RAPTOR). RAPTOR is now deployed as a virtual machine, increasing ease of setup, deployment, and management; increasing system performance; and eliminating the need to ship equipment to and from sites in support of remote assessments.

- Continued to develop processes and integration for Atomic Purple, a framework to integrate advanced persistent threat tactics and insider threat tactics into technical assessments. Standardized remote technical vulnerability scanning and penetration testing capabilities as an additional tool for use during assessments.
- Improved and maintained PowerPedia pages for EA-60, EA-61, and EA-62. Additionally, EA-60 developed an improved EA office discovery template, which is available for all EA offices to add; it is located on the primary EA PowerPedia page.

**Training and certifications:**

Attended the following training:

- DOE Leadership Development Program, 08/12/2020–04/22/2021
    - DOE Leadership Development Program is a professional development opportunity for DOE employees looking to improve their leadership skills and competencies by tailoring leader-level development to individual needs. The program focuses on strategic alignment across all leadership levels to drive transparency and accountability throughout DOE, resulting in an agency positioned for success. Throughout this eight-month program, participants develop critical leadership skills and improve their leadership competency proficiencies.
- SANS training:
    - SEC580: Metasploit Kung Fu for Enterprise Pen Testing
    - FOR578: Cyber Threat Intelligence
    - SEC488: Cloud Security Essentials
    - SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses
    - SEC301: Introduction to Cyber Security
    - SEC573: Automating Information Security with Python
    - MGT512: Security Leadership Essentials for Managers
    - ICS410: ICS/SCADA Security Essentials
    - ICS515: ICS Active Defense and Incident Response
    - ICS456: Essentials for NERC Critical Infrastructure Protection
    - SEC542: Web Application Penetration Testing and Ethical Hacking
- RSA Conference 2021 Virtual Experience, 5/17–5/20, 2021
- Certified Information System Security Professional (Training), 7/26–7/30, 2021
- Offensive Security Certified Professional Study/Lab; Penetration Testing with Kali Linux
- Offensive Security Proving Grounds

- Offensive Security Web Expert Study/Lab; Advanced Web Attacks and Exploitation
- Offensive Security Experienced Penetration Tester Study/Lab; Evasion Techniques and Breaching Defenses

## 6. Appendix B: Legislation, Federal Directives, and Mandates

The Department of Energy (DOE) Cybersecurity Strategy incorporates guiding documents, including Federal mandates and directives to strengthen information sharing and safeguarding. The core list of documents is as follows:

**LEGISLATION, FEDERAL DIRECTIVES, AND MANDATES**

1. National Cyber Strategy (September 2018)
2. Executive Order 13467, Homeland Security Presidential Directive 12 (HSPD-12)
3. Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information
4. Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
5. Executive Order 13870, America's Cybersecurity Workforce (May 2, 2019)
6. Executive Order 13833, Enhancing the Effectiveness of Agency CIOs (May 15, 2018)
7. Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain (May 15, 2019)
8. Executive Order 14028, Improving the Nation's Cybersecurity (March 12, 2021)
9. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources
10. OMB Memorandum M-16-04, OMB Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government
11. OMB Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program
12. OMB Memorandum M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (October 8, 2021)
13. OMB Memorandum M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident (August 27, 2021)
14. OMB Memorandum M-21-30, Protecting Critical Software Through Enhanced Security Measures (August 10, 2021)
15. OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, IM-30 Program Plan, management of reporting and data integrity risk (June 2018)
16. Federal Information Security Modernization Act of 2014 (FISMA)
17. Federal Information Technology Acquisition Reform Act (FITARA)
18. Federal Acquisition Supply Chain Security Act (December 2018)

**DEPARTMENTAL DIRECTIVES, GUIDANCE & SUPPORTING DOCUMENTS**

1. DOE Order 205.1C, Department of Energy Cybersecurity Program
2. NNSA Supplemental Directive 205.1, Baseline Cybersecurity Program
3. DOE Order 206.1, Department of Energy Privacy Program

4. NNSA Supplemental Directive 206.1, Privacy Program
5. DOE Information Resources Management (IRM) Strategic Plan FY 2018-2022
6. Headquarters Facilities Master Security Plan (HQFMSP)
7. Agency Requirement for Physical and Personnel Security and Safeguard Standards
8. DOE Order 472.2, Personnel Security
9. DOE Order 142.3, Unclassified Foreign Visits and Assignments
10. Intelligence Community Standards 703-01 and 703-03
11. Intelligence Community Directives
12. DOE Policy on Implementation of Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain (May 2019)
13. Inspector General Annual FISMA Metrics
14. Intelligence Community Inspector General Annual FISMA Metrics

**DHS DIRECTIVES**

1. Emergency Directive (ED) 21-04 - Mitigate Windows Print Spooler Service Vulnerability
2. ED 21-03 - Mitigate Pulse Connect Secure Product Vulnerabilities
3. ED 21-02 - Mitigate Microsoft Exchange On-Premises Product Vulnerabilities
4. ED 21-01 - Mitigate SolarWinds Orion Code Compromise
5. ED 20-04 - Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday
6. ED 20-03 - Mitigate Windows DNS Server Vulnerability from July 2020 Patch Tuesday
7. ED 20-02 - Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday
8. ED 19-01 - Mitigate DNS Infrastructure Tampering
9. Binding Operational Directive (BOD) 22-01 - Reducing the Significant Risk of Known Exploited Vulnerabilities
10. BOD 20-01 - Develop and Publish a Vulnerability Disclosure Policy
11. BOD 19-02 - Vulnerability Remediation Requirements for Internet-Accessible Systems
12. BOD 18-02 - Securing High Value Assets

**ADDITIONAL SUPPORTING GUIDANCE**

1. National Institute of Standards and Technology (NIST) 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations
2. NIST 800-53B, Control Baselines for Information Systems and Organizations
3. NIST Special Publication (SP) 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
4. NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)
5. NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations
6. NIST SP 800-59, Guideline for Identifying an Information System as a National Security

System

7. NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
8. NIST SP 800-61, Computer Security Incident Handling Guide
9. NIST SP 800-64, Security Considerations in the SDLC
10. NIST SP 800-181 Rev. 1, Workforce Framework for Cybersecurity (National Initiative for Cybersecurity Education Framework)
11. North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)
12. Committee on National Security Systems policies and instructions (e.g., CNSSI 1253 and associated attachments)