U.S. Department of Energy
Washington, D.C.

ORDER

DOE O 227.1A

Approved:12-21-2015

SUBJECT: INDEPENDENT OVERSIGHT PROGRAM

1. PURPOSE. To prescribe the requirements and responsibilities for the Department of Energy (DOE) Independent Oversight Program. The DOE Independent Oversight Program is implemented by the Office of Enterprise Assessments (EA). EA is an independent office within DOE in that it has no line management or policy-making responsibilities or authorities. The Independent Oversight Program comprises one element of DOE's multi-faceted approach to oversight as described in DOE P 226.1, Department of Energy Oversight Policy. Effective oversight, including independent oversight, of DOE federal and contractor operations is an integral part of the Department's responsibility as a self-regulating agency to provide assurance of its safety and security posture to its leadership, its workers, and the public. The Independent Oversight Program is designed to enhance DOE safety and security programs1 by providing the Secretary and Deputy Secretary of Energy, Under Secretaries of Energy, other DOE managers, senior contractor managers, Congress, and other stakeholders with an independent evaluation of the adequacy of DOE policy and requirements, and the effectiveness of DOE and contractor line management performance and risk management in safety and security and other critical functions as directed by the Secretary. The requirements in this directive are designed to ensure that the Independent Oversight Program is implemented in a transparent, efficient, and constructive manner to support the safe and secure accomplishment of DOE's missions.

2. CANCELLATION. DOE O 227.1, *Independent Oversight Program*, dated 8-30-2011. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive. Contractor Requirements Documents (CRDs) that have been incorporated into a contract remain in effect throughout the term of the contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

   a. Departmental Elements. Except as noted in paragraph 3.c., this order applies to all DOE elements, including the National Nuclear Security Administration (NNSA).

      The NNSA Administrator must assure that NNSA employees comply with their responsibilities under this directive. Nothing in this directive will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of

[1] Throughout this directive, safety and security programs means (1) programs for the protection of the public, the environment, and worker health and safety; and (2) programs for the protection of security assets to include special nuclear materials and classified and sensitive unclassified information in all forms. This includes cyber security and emergency management programs.

Public Law (P.L.) 106-65 to establish Administration specific policies, unless disapproved by the Secretary.

b. DOE Contractors. Except for the equivalencies/exemptions in paragraph 3.c., the CRD provided in attachment 1 sets forth requirements of this Order that apply to contracts that include the CRD.

The CRD or its requirements must be included in:

(1) All DOE site/facility management and operating contracts

(2) DOE contracts that contain the clauses Security (Title 48, Code of Federal Regulations (CFR), section 952.204-2), Classification/Declassification (48 CFR 952.204-70), Counterintelligence (48 CFR 970.5204-1), and/or Integration of environment, safety and health into work planning and execution (48 CFR 970.5223-1).

c. Equivalencies/Exemptions. Equivalencies and exemptions to this Order are processed in accordance with DOE O 251.1, *Departmental Directives Program*.

(1) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 USC sections 2406 and 2511 and to ensure consistency through the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.

(2) Exemption. Pursuant to Executive Order 12333, with respect to intelligence-related activities of the Director, Office of Intelligence and Counterintelligence, this Order applies only to information protection (including related physical security measures) and cyber security measures.

4. REQUIREMENTS.

a. Independent Oversight Activities.

(1) EA must conduct independent evaluations (hereafter referred to as Independent Oversight appraisals) of DOE sites, facilities, nuclear design/construction projects, organizations (including DOE Headquarters), and operations to evaluate the effectiveness of DOE and contractor line management performance and risk management in implementing and overseeing safety (nuclear and industrial) and security (cyber and physical) programs, including line oversight and contractor assurance systems (see DOE Order 226.1, *Implementation of Department of Energy*

Oversight Policy). EA must also evaluate the adequacy of DOE policy, and other critical functions when directed by the Secretary.

(2) EA must evaluate performance and management of safety and security risks against applicable laws, statutes, rules, executive orders, national standards, DOE directives, DOE-approved plans and program documents (e.g., security plans, emergency plans, authorization basis documents, worker safety and health programs, quality assurance program plans), site-specific procedures, and contractual requirements. This includes requirements promulgated by Program Secretarial Officers and formally authorized for use by organizations under their cognizance.

(3) EA must use a formal documented process to manage and conduct Independent Oversight appraisals that is published and accessible to DOE employees. This process is provided in the *Independent Oversight Appraisal Process Protocols* available at http://energy.gov/ea/services/assessments.

(4) Independent Oversight appraisals must be prioritized on areas of greatest potential risks and implemented in a manner that supports DOE line management in accomplishing its line management oversight and achieving DOE mission objectives safely and securely. Higher priority and greater emphasis is placed on conducting Independent Oversight appraisals of high consequence activities, such as nuclear project design, construction and commissioning; high hazard nuclear operations; protection of high value security assets (e.g., Category I quantities of special nuclear material and classified information assets, including special access programs, Sensitive Compartmented Information, and such Restricted Data Sigma categories as 14, 15, 18, and 20); DOE systems and assets that are critical infrastructure as defined by Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience*; systems or programs that can have widespread impacts (e.g., interconnected computer networks); and Independent Oversight appraisals required by other DOE directives. Other areas of consideration for Independent Oversight appraisals are organizations whose performance may present significant risk (e.g., less than expected safety or security performance records and/or serious or recurring incidents or violations of requirements).

(5) Persons who perform Independent Oversight appraisals must be technically qualified and knowledgeable in the areas they assess.

(6) EA will encourage managers from the line organization subject to an appraisal to observe appraisal activities. EA will encourage and accommodate appraisal augmentees from other organizations whenever feasible (see the *Independent Oversight Appraisal Process Protocols*).

b. Licensed DOE Facilities or Activities. Independent Oversight appraisal activities for DOE facilities or activities licensed by the Nuclear Regulatory Commission must, except where excluded by law or DOE policy, be structured to minimize or eliminate duplication of oversight efforts while ensuring DOE safety and security programs and associated facilities are independently evaluated. Accordingly, the scheduling of independent oversight activities must take into account the inspection and assessment activities of the Nuclear Regulatory Commission.

c. Appraisal Planning.

(1) Independent Oversight appraisal activities must be coordinated with affected DOE line management and staff offices to promote efficient and effective use of resources. EA appraisal schedules will take into consideration Program Office and Field Element assessment plans and schedules. Disagreements regarding scheduling appraisals that cannot be resolved between the cognizant EA Office Director and cognizant manager must be elevated through organizational management levels up to and including the Deputy Secretary for resolution.

(2) EA will issue an appraisal plan before each appraisal that communicates the scope, schedule, and team composition for the appraisal to the line management of the organization subject to the appraisal, to include representatives of the applicable Program Office and Field Element. In some cases, an appraisal plan may cover a series of related appraisals at a site or similar appraisals to be conducted at multiple sites. EA must notify the cognizant DOE line management if circumstances or conditions are identified that necessitate deviating from the documented scope of the appraisal and coordinate with line management to accommodate the revised scope.

(3) Upon EA request, DOE and contractor management must provide access to facilities, managers and staff, and documents or other data. EA will tailor document requests to the specific information needed to support the established scope of the appraisal. Organizations subject to appraisals must identify access requirements (e.g., security, training, personal protective equipment) with sufficient lead time to allow Independent Oversight personnel to gain prompt access to sites, facilities, and/or networks at the onset of an appraisal.

(4) EA must assure that appraisal team members have no conflict of interest or appearance of conflict of interest with the subjects they review.

(5) Select Independent Oversight appraisal activities require Federal and contractor representatives to serve as trusted agents. Trusted agents assist in planning and conducting performance tests, and must accomplish this without divulging or compromising sensitive testing information. The number of trusted agents representing the site or organization must be kept

to the absolute minimum, and trusted agents must have the authority to make decisions regarding testing details on behalf of their facility/organization. To support safe and credible oversight activities, EA will coordinate performance test scenarios with appropriate trusted agents. For safeguards and security performance tests, this will include coordination with the Officially Designated Federal Security Authority (ODFSA) or his/her designee.

(6) EA's performance test scenarios for force-on-force security exercises support its independent assessment of the adequacy of a site's protection strategy and response plan execution, and are based upon the Department's threat policy. EA will routinely conduct performance testing using scenarios representing baseline adversary threat levels and capabilities against which possessing sites are expected to achieve high system effectiveness. After coordination with the ODFSA, EA may conduct additional performance tests based on scenarios that exceed established baseline adversary threat levels and capabilities in order to maintain awareness of potential security system vulnerabilities should the threat environment change in the future. EA and ODFSA representatives will work collaboratively to plan safe and operationally credible security exercises that achieve the established test objectives and minimize exercise artificialities. Safety concerns will be resolved before a security exercise is performed. ODFSA disagreements with the credibility of EA performance test scenarios (both at and above baseline threat levels and capabilities) must be elevated through organizational management levels (up to the Deputy Secretary if necessary) until resolution is obtained. EA oversight reports will clearly delineate the nature of each performance test conducted.

(7) Most Independent Oversight appraisals are announced in advance to the responsible DOE and contractor organization to promote effective coordination and efficient resource utilization. Where EA determines that unannounced appraisals are necessary to evaluate safety and security performance (e.g., cyber security penetration testing, limited notice performance testing of critical physical and information security controls), trusted agents from responsible DOE Program Offices and Field Elements must be consulted in advance and kept informed as the unannounced appraisal is conducted. Safety and security considerations are paramount in planning and conducting unannounced appraisals.

d. Conduct of Appraisals.

(1) The EA appraisal team leader must provide informal written (preferable) or verbal information on preliminary observations from the appraisal to line management’s designee at the conclusion of onsite data collection activities.

(2) EA must document all of its Independent Oversight appraisals. The appraisal documentation must identify the overall effectiveness of the DOE and/or contractor organization in managing the appraised functions and any "findings" that represent risks to the mission and warrant a high level of management attention. EA appraisal documents may also list specific implementation "deficiencies"; suggested "opportunities for improvement" to assist cognizant managers in improving programs and operations; any identified "best practices" that could help other DOE organizations solve challenging problems; and "recommendations" for senior line management's consideration for improving program or management effectiveness (see Definitions in Appendix 1). Findings and deficiencies must reference applicable requirements to facilitate disposition by the site's or program's issues management system. Appraisals may also identify ratings (e.g., effective performance, needs improvement, or significant weakness) where appropriate to convey the appraisal results.

(3) The factual accuracy of appraisal results must be verified by the cognizant DOE management responsible for the program or activity. For major appraisals (e.g., multi-topic inspections), the results will be provided to the cognizant DOE Field Element and Program Office for factual accuracy review. Disagreements regarding the factual accuracy of the appraisal results or findings that cannot be resolved between the cognizant EA Office Director and the cognizant manager must be elevated through organizational management levels up to and including the Deputy Secretary for resolution and must consider any relevant interpretation of the requirements issued by the cognizant OPI for the directive.

(4) For major Independent Oversight appraisals, EA must provide the cognizant Program Secretarial Officer the opportunity to submit a written management response to the conclusions and any recommendations included in the final draft appraisal report. If provided, EA will reflect this response in an appendix to the final appraisal report.

(5) EA must coordinate with the affected cognizant Program Secretarial Officers, DOE Field Elements, and Under Secretaries before briefing other DOE personnel on appraisal results. EA must coordinate with the affected DOE organizations and the Departmental Representative to the Defense Nuclear Facilities Safety Board (DNFSB) before briefing the DNFSB. In both situations, the secretarial officer and/or DOE Field Element manager must be offered the opportunity to address the appraisal outcomes, which may be accomplished verbally and/or in writing.

e. Response to Major Vulnerabilities or Imminent Danger.

(1) EA personnel must notify the cognizant DOE manager verbally as soon as possible and provide written notification within 24 hours when appraisal activities indicate either of the following conditions:

(a) an imminent danger or condition that presents an unacceptable immediate risk to workers, public health, or the environment, or

(b) a major vulnerability (e.g., unacceptable risk of special nuclear material theft or diversion, radiological or industrial sabotage, espionage, or significant compromise of classified information).

(2) When notified of either of the above conditions, cognizant DOE management must take actions to mitigate the short and long-term risk, and must notify the Program Secretarial Officer and EA within 10 working days of actions taken and any compensatory measures planned.

(3) If the cognizant DOE management disagrees with EA's characterization of the severity of the identified condition or the need for prompt action, this must immediately be brought to the attention of the Program Secretarial Officer or Under Secretary as applicable, and EA Director for resolution.

f. Corrective Actions.

(1) Corrective action plans must be developed and implemented for Independent Oversight appraisal findings. Cognizant DOE managers must use site- and program-specific issues management processes and systems developed in accordance with DOE O 226.1 to manage and approve these corrective action plans and track them to completion. For findings and corrective actions pertaining to safeguards and security (excluding cyber security) activities, the DOE Safeguards and Security Information Management System (SSIMS) must be used for this purpose (reference DOE O 470.4, *Safeguards and Security Program*). Findings and other deficiencies identified in Independent Oversight appraisal reports are managed in accordance with DOE O 226.1 processes and Quality Assurance Programs established to meet the requirements of DOE O 414.1, *Quality Assurance,* and 10 CFR Part 830, *Nuclear Safety Management*.

(2) At the discretion of the EA Director, or when requested by the cognizant DOE manager, EA must review the adequacy of proposed corrective action plans developed in response to appraisal results and provide comments for consideration.

(3) EA must establish and implement a tailored approach for following up on findings based on significance and complexity. The approach must include selected appraisals to review the timeliness and adequacy of corrective actions, verify and validate the effectiveness of the corrective actions, and confirm closure of findings.

(4) Cognizant DOE managers must provide EA with information on corrective actions related to prior Independent Oversight appraisals of their organization, sites, and/or contractor activities when requested.

(5) Disagreements regarding the adequacy or effectiveness of corrective actions that cannot be resolved between the cognizant EA Office Director and the cognizant DOE manager must be elevated through organizational management levels until resolution is obtained. If needed, issues must be elevated to the Deputy Secretary for resolution.

5. RESPONSIBILITIES.

a. Program Secretarial Officers, including the NNSA Administrator. [2]

(1) Where appropriate, review and provide comments on the factual accuracy of draft appraisal reports.

(2) Take timely and appropriate action to address findings identified in Independent Oversight appraisal reports and approve corrective action plans as appropriate. Address other deficiencies identified in Independent Oversight appraisal reports in accordance with established issues management processes (DOE O 226.1) and quality assurance programs (DOE O 414.1).

(3) Provide EA with requested documentation, points of contact, and access to sites, facilities, networks, and operations in support of appraisal activities.

(4) Work with the EA Director to resolve disagreements on appraisal schedules, appraisal results, or findings that are unable to be resolved at lower organizational levels. Escalate those issues to the Deputy Secretary, if necessary, to achieve resolution.

(5) Ensure that appraisal findings and corrective actions pertaining to safeguards and security (excluding cyber security) activities are entered into SSIMS.

b. Director, Office of Enterprise Assessments.

(1) Direct and manage the safety and security Independent Oversight Program.

(2) Develop and maintain documents that describe the safety and security Independent Oversight Program and implementing methods.

[2] In most cases, the program secretarial officer is also the lead program secretarial officer for a site or facility. If the program secretarial officer is not also the lead program secretarial officer, the program secretarial officer is responsible for coordinating with the lead program secretarial officer on any findings that require input or action from the lead program secretarial officer.

(3) Ensure that senior EA management oversight is provided for all appraisal planning, conduct, and reporting.

(4) Determine the appropriate distribution of appraisal reports, to include applicable Program Office representatives and Heads of Field Elements, and lessons learned information resulting from appraisals.

(5) Provide updates, as appropriate, on the status of appraisals to the Secretary, Deputy Secretary, Under Secretaries, Program Secretarial Officers, and applicable Offices of Primary Interest (OPI) for DOE directives.

(6) Brief senior DOE officials, including the NNSA Administrator, Under Secretaries, Program Secretarial Officers, OPI managers, Heads of Field Elements, and senior representatives of affected contractors on the results of appraisal activities where appropriate.

(7) Notify the DOE Inspector General when appraisal activities identify concerns involving potential criminal activities and/or waste, fraud, and abuse.

(8) Work with Program Secretarial Officers to resolve disagreements on appraisal schedules, appraisal results, or findings that are unable to be resolved at lower organizational levels. Escalate those issues to the Deputy Secretary, if necessary, to achieve resolution.

(9) Direct and manage the National Training Center (NTC) to ensure lessons learned from Independent Oversight activities are integrated into NTC safety and security training courses.

(10) Notify the applicable Program Secretarial Officer when findings identified by EA have not been resolved effectively or in a timely manner.

c. Directors, Office of Cyber and Security Assessments and Office of Environment, Safety and Health Assessments.

(1) Coordinate the scheduling, notification, and planning of appraisal activities with appropriate Program Secretarial Officers and/or Heads of Field Elements.

(2) Ensure that appraisal teams are comprised of an appropriate number of qualified personnel and are effectively supervised during planning, conduct and reporting of appraisal results.

(3) Coordinate with the applicable OPIs to ensure accurate understanding of requirements related to safety and security findings and deficiencies identified during appraisals.

(4) Formally notify the applicable OPI when inadequacies relating to DOE policy or DOE directives are identified.

(5) Post the title and date of all final appraisal reports on the appropriate EA website. Post a copy of final appraisal reports that do not contain or reveal classified or controlled unclassified information.

d. Director, Office of Cyber and Security Assessments.

(1) In addition to other cyber security appraisal activities, conduct appraisals of DOE national security systems, including national security systems processing intelligence information, to meet the annual independent evaluation requirements of the Federal Information Security Management Act.

(2) Perform the annual evaluation of security vulnerabilities on NNSA national laboratory computers for submittal to the National Counterintelligence Policy Board.

(3) Coordinate with the Office of the Chief Information Officer, as the Office of Primary Interest, and provide annual briefings to the DOE Cyber Council regarding the tracking of findings and resolution of issues across the enterprise.

e. Heads of Field Elements.[3]

(1) Identify contracts to which the CRD requirements should apply and notify the cognizant contracting officers.

(2) Review and comment on the factual accuracy of draft appraisal reports.

(3) Take timely and appropriate action to address the findings identified in Independent Oversight appraisal reports and approve corrective action plans as appropriate. Address other deficiencies identified in Independent Oversight appraisal reports in accordance with established issues management processes (DOE O 226.1) and quality assurance programs (DOE O 414.1).

(4) Provide EA with requested documentation, points of contact, and information concerning programs under their jurisdiction; ensure necessary support for appraisal activities, including access to sites, facilities, networks, and operations; and provide work space for appraisal teams.

[3] Operations offices, service centers, site offices, field offices, area offices, production offices, project management offices, government-owned government-operated facilities and regional offices of federally-staffed laboratories that report directly to a DOE Headquarters office.

f. Contracting Officers. Incorporate the CRD into contracts in a timely fashion upon notification of its applicability. If delegated the authority from the Head of the Field Element, the contracting officer may incorporate equivalent contract clauses or requirements into contracts in lieu of the CRD.

g. Executive Secretary of the Special Access Program Oversight Committee. Assist EA in obtaining access to special access programs as required to provide effective independent oversight of the overall DOE security program.

h. Offices of Primary Interest (for DOE Directives).

(1) As applicable, review and comment on the factual accuracy of draft Independent Oversight appraisal reports.

(2) Evaluate inadequacies in DOE policies, DOE directives, or activities of the OPI that are identified and transmitted by EA. Document decisions on the need for corrective actions and track all actions to closure.

(3) Provide clarification regarding requirements contained in DOE directives under their cognizance and issue written authoritative interpretations of such requirements when necessary or when requested by EA or a DOE line organization.

6. REFERENCES.

a. DOE P 226.1, *Department of Energy Oversight Policy*, which establishes DOE's expectations for implementation of a comprehensive and robust oversight process.

b. DOE O 226.1, *Implementation of Department of Energy Oversight Policy*, which establishes requirements and provides direction for implementing DOE P 226.1.

c. DOE O 251.1, *Departmental Directives Program*, which establishes requirements and responsibilities for implementing the DOE Directives Program.

d. DOE O 414.1, *Quality Assurance*, which establishes requirements for ensuring that DOE work meets requirements and expectations, and that quality improvement is effected through rigorous assessments and effective corrective actions.

e. DOE O 470.4, *Safeguards and Security Program*, which establishes requirements and responsibilities for managing DOE safeguards and security programs, including managing safeguards and security-related corrective actions.

f. Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience*, which establishes a national policy and Federal government roles and responsibilities for strengthening the security and resilience of United States critical infrastructure against physical and cyber threats.

g. 10 CFR Part 830, *Nuclear Safety Management*, which establishes requirements for the conduct of activities that may affect the safety of DOE nuclear facilities.

7. DEFINITIONS. See Appendix 1.

8. CONTACT. Questions concerning this Order should be directed to the Office of Enterprise Assessments at 202-586-0271.

BY ORDER OF THE SECRETARY OF ENERGY:

ELIZABETH SHERWOOD-RANDALL
Deputy Secretary

DEFINITIONS

Appraisal: An appraisal is an Independent Oversight activity conducted by the Office of Enterprise Assessments to evaluate the effectiveness of line management performance and risk management or the adequacy of DOE policies and requirements.

Best Practice: A best practice is a safety or security-related practice, technique, process, or program attribute observed during an appraisal that may merit consideration by other DOE and contractor organizations for implementation because it: (1) has been demonstrated to substantially improve safety or security performance of a DOE operation; (2) represents or contributes to superior performance (beyond compliance); (3) solves a problem or reduces the risk of a condition or practice that affects multiple DOE sites or programs; or (4) provides an innovative approach or method to improve effectiveness or efficiency.

Cognizant Manager: The DOE field or Headquarters manager who is directly responsible for program management and direction, and the development and implementation of corrective actions. Cognizant managers may be line managers or managers of support organizations.

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

Directives: Directives are defined in DOE O 251.1, *Departmental Directives Program*.

Findings: Findings are deficiencies that warrant a high level of attention on the part of management. If left uncorrected, findings could adversely affect the DOE mission, the environment, worker safety or health, the public or national security. Findings define the specific nature of the deficiency, whether it is localized or indicative of a systemic problem, and identify which organization is responsible for corrective actions.

Imminent Danger: Conditions or practices in the workplace where a danger exists which could reasonably be expected to cause death or serious physical harm either immediately or before the abatement of such danger, through normal procedures, would otherwise be required.

Independent Oversight: Independent oversight refers exclusively to oversight by DOE Headquarters organizations that do not have line management responsibility for the activity. Oversight by supporting organizations that are direct reports to line management is not considered DOE independent oversight. Within DOE, the sole responsibility for independent oversight of safety and security programs resides with the Office of Enterprise Assessments, reporting directly to the Office of the Secretary of Energy.

Line Management: Line management refers the unbroken chain of responsibility that extends from the Secretary of Energy to the Deputy Secretary, to the Secretarial Officers who set program policy and plans and develop assigned programs, to the program and Field Element Managers, and to the contractors and subcontractors who are responsible for execution of these programs. It is distinct from DOE support organizations, such as the Office of Environment,

Health, Safety and Security, Office of Management, and Office of the Chief Information Officer, which also have responsibilities and functions important to security and safety.

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

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

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

Policy: The term "DOE policy" or "policy" when used in lower case in this Order is meant to be all inclusive of documents describing the philosophies, fundamental values, administration, requirements, and expectations for operation of the Department. It includes but is not limited to DOE Policies and other types of directives issued under DOE O 251.1.

Program Secretarial Officers: Heads of DOE Departmental Elements listed on the Office of Management website at https://www.directives.doe.gov/references/doe_departmental_elements.

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

Safety and security programs: Includes (1) programs for the protection of the public, the environment, and worker health and safety; and (2) programs for the protection of security assets to include special nuclear materials and classified and sensitive unclassified information in all forms. Within the scope of this directive, safety and security programs include cyber security and emergency management programs.

CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 227.1A, *Independent Oversight Program*

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements.

The contractor must meet the following requirements:

1. The contractor must support the conduct of Independent Oversight appraisal activities conducted by the Office of Enterprise Assessments (EA) at sites and facilities for which they are responsible. This support includes, but is not limited to, providing the following:

    a. timely identification of points of contact to provide information and support during appraisals;

    b. documentation and information concerning safety and security programs[4] for which they are responsible;

    c. access to contractor-managed facilities, networks, and personnel; and

    d. work space and administrative support for appraisal teams.

2. When notified by EA of an imminent danger or condition or major vulnerability that presents an unacceptable immediate risk to workers, the public, the environment, or national security, the responsible contractor organization must take the following actions in coordination with DOE line management:

    a. promptly identify and implement immediate compensatory actions to mitigate the condition,

    b. within 5 working days, notify the cognizant DOE line manager of actions taken and compensatory measures planned, and

    c. develop and implement actions (including determining costs and identifying funds) to eliminate the vulnerability or reduce the level of risk to an acceptable level as soon as possible.

3. When requested, the contractor must review and provide comments on the factual accuracy of draft appraisal reports through the responsible DOE field element.

[4] Throughout this document, safety and security programs means (1) programs for the protection of the public, the environment, and worker health and safety; and (2) programs for the protection of security assets to include special nuclear materials and classified and sensitive unclassified information in all forms. This includes cyber security and emergency management programs.

4. Draft appraisal reports provided to contractors for review must only be shared with personnel within their organization, parent corporations, and subcontractors for the purpose of factual accuracy evaluation and initial corrective action development and implementation.

5. The contractor must prepare, implement, and track to completion corrective actions to address findings identified in EA appraisal reports. Findings and other deficiencies identified in appraisal reports are managed in accordance with established issues management systems (DOE O 226.1) and quality assurance programs (DOE O 414.1 and 10 CFR Part 830).

6. The contractor must provide information on corrective actions to DOE when requested to support EA appraisal activities.