

## Presidential Documents

Executive Order 13587 of October 7, 2011

### Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to ensure the responsible sharing and safeguarding of classified national security information (classified information) on computer networks, it is hereby ordered as follows:

**Section 1. Policy.** Our Nation's security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management.

This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.

#### **Sec. 2. General Responsibilities of Agencies.**

**Sec. 2.1.** The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks. As part of this responsibility, they shall:

(a) designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts for the agency;

(b) implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order;

(c) perform self-assessments of compliance with policies and standards issued pursuant to sections 3.3, 5.2, and 6.3 of this order, as well as other applicable policies and standards, the results of which shall be reported annually to the Senior Information Sharing and Safeguarding Steering Committee established in section 3 of this order;

(d) provide information and access, as warranted and consistent with law and section 7(d) of this order, to enable independent assessments by the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force of compliance with relevant established policies and standards; and

(e) detail or assign staff as appropriate and necessary to the Classified Information Sharing and Safeguarding Office and the Insider Threat Task Force on an ongoing basis.

**Sec. 3. Senior Information Sharing and Safeguarding Steering Committee.**

**Sec. 3.1.** There is established a Senior Information Sharing and Safeguarding Steering Committee (Steering Committee) to exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks.

**Sec. 3.2.** The Steering Committee shall be co-chaired by senior representatives of the Office of Management and Budget and the National Security Staff. Members of the committee shall be officers of the United States as designated by the heads of the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Information Security Oversight Office within the National Archives and Records Administration (ISOO), as well as such additional agencies as the co-chairs of the Steering Committee may designate.

**Sec. 3.3.** The responsibilities of the Steering Committee shall include:

(a) establishing Government-wide classified information sharing and safeguarding goals and annually reviewing executive branch successes and shortcomings in achieving those goals;

(b) preparing within 90 days of the date of this order and at least annually thereafter, a report for the President assessing the executive branch's successes and shortcomings in sharing and safeguarding classified information on computer networks and discussing potential future vulnerabilities;

(c) developing program and budget recommendations to achieve Government-wide classified information sharing and safeguarding goals;

(d) coordinating the interagency development and implementation of priorities, policies, and standards for sharing and safeguarding classified information on computer networks;

(e) recommending overarching policies, when appropriate, for promulgation by the Office of Management and Budget or the ISOO;

(f) coordinating efforts by agencies, the Executive Agent, and the Task Force to assess compliance with established policies and standards and recommending corrective actions needed to ensure compliance;

(g) providing overall mission guidance for the Program Manager-Information Sharing Environment (PM-ISE) with respect to the functions to be performed by the Classified Information Sharing and Safeguarding Office established in section 4 of this order; and

(h) referring policy and compliance issues that cannot be resolved by the Steering Committee to the Deputies Committee of the National Security Council in accordance with Presidential Policy Directive/PPD-1 of February 13, 2009 (Organization of the National Security Council System).

**Sec. 4. Classified Information Sharing and Safeguarding Office.**

**Sec. 4.1.** There shall be established a Classified Information Sharing and Safeguarding Office (CISSO) within and subordinate to the office of the PM-ISE to provide expert, full-time, sustained focus on responsible sharing and safeguarding of classified information on computer networks. Staff of the CISSO shall include detailees, as needed and appropriate, from agencies represented on the Steering Committee.

**Sec. 4.2.** The responsibilities of CISSO shall include:

(a) providing staff support for the Steering Committee;

(b) advising the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force on the development of an effective program to monitor compliance with established policies

and standards needed to achieve classified information sharing and safeguarding goals; and

(c) consulting with the Departments of State, Defense, and Homeland Security, the ISOO, the Office of the Director of National Intelligence, and others, as appropriate, to ensure consistency with policies and standards under Executive Order 13526 of December 29, 2009, Executive Order 12829 of January 6, 1993, as amended, Executive Order 13549 of August 18, 2010, and Executive Order 13556 of November 4, 2010.

**Sec. 5. *Executive Agent for Safeguarding Classified Information on Computer Networks.***

**Sec. 5.1.** The Secretary of Defense and the Director, National Security Agency, shall jointly act as the Executive Agent for Safeguarding Classified Information on Computer Networks (the “Executive Agent”), exercising the existing authorities of the Executive Agent and National Manager for national security systems, respectively, under National Security Directive/NSD–42 of July 5, 1990, as supplemented by and subject to this order.

**Sec. 5.2.** The Executive Agent’s responsibilities, in addition to those specified by NSD–42, shall include the following:

(a) developing effective technical safeguarding policies and standards in coordination with the Committee on National Security Systems (CNSS), as re-designated by Executive Orders 13286 of February 28, 2003, and 13231 of October 16, 2001, that address the safeguarding of classified information within national security systems, as well as the safeguarding of national security systems themselves;

(b) referring to the Steering Committee for resolution any unresolved issues delaying the Executive Agent’s timely development and issuance of technical policies and standards;

(c) reporting at least annually to the Steering Committee on the work of CNSS, including recommendations for any changes needed to improve the timeliness and effectiveness of that work; and

(d) conducting independent assessments of agency compliance with established safeguarding policies and standards, and reporting the results of such assessments to the Steering Committee.

**Sec. 6. *Insider Threat Task Force.***

**Sec. 6.1.** There is established an interagency Insider Threat Task Force that shall develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within agencies.

**Sec. 6.2.** The Task Force shall be co-chaired by the Attorney General and the Director of National Intelligence, or their designees. Membership on the Task Force shall be composed of officers of the United States from, and designated by the heads of, the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the ISOO, as well as such additional agencies as the co-chairs of the Task Force may designate. It shall be staffed by personnel from the Federal Bureau of Investigation and the Office of the National Counterintelligence Executive (ONCIX), and other agencies, as determined by the co-chairs for their respective agencies and to the extent permitted by law. Such personnel must be officers or full-time or permanent part-time employees of the United States. To the extent permitted by law, ONCIX shall provide an appropriate work site and administrative support for the Task Force.

**Sec. 6.3.** The Task Force’s responsibilities shall include the following:

(a) developing, in coordination with the Executive Agent, a Government-wide policy for the deterrence, detection, and mitigation of insider threats, which shall be submitted to the Steering Committee for appropriate review;

(b) in coordination with appropriate agencies, developing minimum standards and guidance for implementation of the insider threat program's Government-wide policy and, within 1 year of the date of this order, issuing those minimum standards and guidance, which shall be binding on the executive branch;

(c) if sufficient appropriations or authorizations are obtained, continuing in coordination with appropriate agencies after 1 year from the date of this order to add to or modify those minimum standards and guidance, as appropriate;

(d) if sufficient appropriations or authorizations are not obtained, recommending for promulgation by the Office of Management and Budget or the ISOO any additional or modified minimum standards and guidance developed more than 1 year after the date of this order;

(e) referring to the Steering Committee for resolution any unresolved issues delaying the timely development and issuance of minimum standards;

(f) conducting, in accordance with procedures to be developed by the Task Force, independent assessments of the adequacy of agency programs to implement established policies and minimum standards, and reporting the results of such assessments to the Steering Committee;

(g) providing assistance to agencies, as requested, including through the dissemination of best practices; and

(h) providing analysis of new and continuing insider threat challenges facing the United States Government.

**Sec. 7. General Provisions.** (a) For the purposes of this order, the word "agencies" shall have the meaning set forth in section 6.1(b) of Executive Order 13526 of December 29, 2009.

(b) Nothing in this order shall be construed to change the requirements of Executive Orders 12333 of December 4, 1981, 12829 of January 6, 1993, 12968 of August 2, 1995, 13388 of October 25, 2005, 13467 of June 30, 2008, 13526 of December 29, 2009, 13549 of August 18, 2010, and their successor orders and directives.

(c) Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; the Secretary of Defense under Executive Order 12829, as amended; the Secretary of Homeland Security under Executive Order 13549; the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; the Director of ISOO under Executive Orders 13526 and 12829, as amended; the PM-ISE under Executive Order 13388 or the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; the Director, Central Intelligence Agency under NSD-42 and Executive Order 13286, as amended; the National Counterintelligence Executive, under the Counterintelligence Enhancement Act of 2002; or the Director of National Intelligence under the National Security Act of 1947, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, NSD-42, and Executive Orders 12333, as amended, 12968, as amended, 13286, as amended, 13467, and 13526.

(d) Nothing in this order shall authorize the Steering Committee, CISSO, CNSS, or the Task Force to examine the facilities or systems of other agencies, without advance consultation with the head of such agency, nor to collect information for any purpose not provided herein.

(e) The entities created and the activities directed by this order shall not seek to deter, detect, or mitigate disclosures of information by Government employees or contractors that are lawful under and protected by the Intelligence Community Whistleblower Protection Act of 1998, Whistleblower

Protection Act of 1989, Inspector General Act of 1978, or similar statutes, regulations, or policies.

(f) With respect to the Intelligence Community, the Director of National Intelligence, after consultation with the heads of affected agencies, may issue such policy directives and guidance as the Director of National Intelligence deems necessary to implement this order.

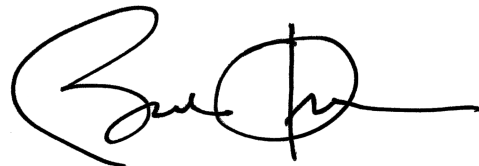
(g) Nothing in this order shall be construed to impair or otherwise affect:

(1) the authority granted by law to an agency, or the head thereof; or

(2) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(h) This order shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(i) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

A handwritten signature in black ink, appearing to be Barack Obama's signature, consisting of a large 'B' followed by a circle and a horizontal line.

THE WHITE HOUSE,  
*October 7, 2011.*

**SUBJECT: INSIDER THREAT PROGRAM**

---

1. PURPOSE. To establish responsibilities and requirements for the Department of Energy (DOE) Insider Threat Program (ITP). The purpose of the ITP is to deter, detect, and mitigate insider threat actions by Federal and contractor employees in accordance with the requirements of Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, dated October 7, 2011, the *National Insider Threat Policy* (“National Policy”) and *Minimum Standards for Executive Branch Insider Threat Programs* (“Minimum Standards”), dated November 21, 2012, and other government-wide and DOE requirements. The ITP applies to all programs in an integrated manner that may address threats to personnel, facilities, material (e.g., special nuclear material), information, equipment and other DOE or other United States Government assets. This directive establishes a central ITP for DOE. Any conflict with other DOE Directives or requirements should be reported to the Department’s senior insider threat official for resolution.
2. CANCELLATION. None.
3. APPLICABILITY.
  - a. Departmental Elements.
    - (1) Except as otherwise indicated in this section, the requirements in this Order apply to all Departmental Elements. Direction to National Nuclear Security Administration (NNSA) personnel and programs will be effected through the Secretary of Energy, the Deputy Secretary of Energy, or will otherwise comply with the NNSA Act.
    - (2) The Administrator of the NNSA must ensure 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 the NNSA Act (“NNSA Act”) (50 United States Code (U.S.C.) § 2402(d)) to establish Administration-specific policies, unless disapproved by the Secretary.
    - (3) This Order applies to the Bonneville Power Administration (BPA). The BPA Administrator will assure that BPA employees and contractors comply with their respective responsibilities under this directive consistent with BPA’s self-financing, procurement and other statutory authorities.
    - (4) The requirements in this Order apply to DOE (and DOE contractor) activities and facilities that are subject to licensing and related regulatory authority or certification by the Nuclear Regulatory Commission (NRC). The requirements in this Order should be applied consistent with Executive Order 12829, "Executive National Industrial Security Program"

(January 6, 1993), the 1996 “Memorandum of Understanding Between the U.S. Department of Energy and the U.S. Nuclear Regulatory Commission Under the Provisions of the National Industrial Security Program” as may be amended or superseded, and related memoranda of understanding between NRC and DOE concerning classified information, executed in accordance with applicable laws, regulations, policies, directives, and requirements.

- b. DOE Contractors. Except for the equivalencies/exemptions in paragraph 3.c., the Contractor Requirements Document (CRD) (Attachment 1) sets forth requirements of this Order that will apply to contracts that include the CRD.

The CRD must be included in all contracts that involve cleared employees, classified information or matter, Special Nuclear Material, nuclear weapons or parts, or contain DOE Acquisition Regulation (DEAR) clause 952.204-2, *Security Requirements*.

A violation of the provisions of the CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to section 234B of the Atomic Energy Act (42 U.S.C. Section 2282b). The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations (CFR), Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*.

- c. Equivalencies/Exemptions for DOE O 470.5. Equivalencies and exemptions from the requirements of this Order are processed in accordance with DOE O 251.1C, *Departmental Directives Program*.

- (1) Equivalencies or exemptions from the requirements in this Order must be supported by sufficient analysis to form the basis for an informed risk management decision. The analysis must identify compensatory measures, if applicable, or alternative controls to be implemented.
- (2) All approved equivalencies and exemptions under this Order must be entered in the Safeguards and Security Information Management System (SSIMS) database and incorporated into the affected security or other plan(s). Approved equivalencies and exemptions become a valid basis for operation when they have been entered in SSIMS and documented in the appropriate plan, and they must be incorporated into local procedures at that time.
- (3) Many DOE ITP requirements are found in or based on regulations issued by Federal agencies, and codified in the CFR or other authorities, such as Executive Orders or Presidential Directives. In such cases, the process for deviating from those requirements found in the source document must be applied. If the source document does not include a deviation process, the DOE Office of the General Counsel, or NNSA Office of the General

Counsel if an NNSA element is involved, must be consulted to determine whether and how deviation from the source can be legally pursued.

- (4) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344 (February 1, 1982), codified at 50 U.S.C. Sections 2406 and 2511, and to ensure consistency throughout 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.

#### 4. REQUIREMENTS.

- a. An ITP must be developed and maintained to deter, detect, mitigate, analyze and respond to insider threats.
- b. The ITP must:
  - (1) Fulfill and maintain consistency with the National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs;
  - (2) Identify insider threats and take appropriate actions to deter them from causing damage to DOE personnel, resources, capabilities and national security commensurate with the potential consequences of the insider threats' access, intent and ability;
  - (3) Ensure legal, civil and privacy rights and civil liberties are preserved and protected;
  - (4) Integrate insider threat related policies, procedures and resources across DOE, that include counterintelligence, security, human capital, legal counsel, information management and other DOE Elements that can contribute to deterring, identifying and managing insider threats;
  - (5) Identify, collect and process data required to identify and address insider threats;
  - (6) Coordinate insider threat analysis, response and mitigation actions with appropriate law enforcement agencies, DOE intelligence, security, legal counsel, inspector general, human capital and other cognizant organizations;
  - (7) Establish, maintain and conduct training or awareness activities to ensure all cleared Federal and contractor employees are informed of their responsibilities and provided required information related to the ITP; and
  - (8) Monitor user activity on classified networks.



- c. DOE sites, facilities, programs and personnel must provide or provide access to data as required for the ITP to successfully execute its mission.
- d. DOE programs must identify the resources to support the ITP and provide this information to the ITP Working Group (ITPWG).
- e. Annual progress/status reports must be prepared for the Secretary of Energy through the ITPWG and the Senior Information Sharing and Safeguarding Steering Committee (SISSSC) established by E.O. 13587 to document and report the progress/status of the ITP.
- f. DOE information system usage banners, policies and user agreements must be approved according to Designated Senior Official (DSO) direction and in consultation with the Office of the General Counsel.
- g. Senior Counterintelligence Officers must ensure that Local Insider Threat Working Groups (LITWG) are established.
- h. Documentation pursuant to the ITP must be reviewed for classified and controlled unclassified information and handled accordingly.
- i. DSO-approved insider threat detection, assessment and referral criteria and procedures must be documented.
- j. Data sources and format(s) needed to support the centralized analytic operations must be documented.

5. RESPONSIBILITIES.

- a. Secretary of Energy.
  - (1) Establishes, directs and maintains an effective ITP in accordance with Executive Order 13587 and other national directives and policies.
  - (2) Designates the senior official to lead and coordinate the ITP.
  - (3) Establishes the ITP Executive Steering Committee (ESC).
- b. Designated Senior Official (DSO).
  - (1) Advises and reports directly to the Secretary of Energy and Deputy Secretary of Energy regarding the planning, construct and operation of the ITP.
  - (2) Provides management, direction, guidance and oversight of the ITP in accordance with Section 3.a. (1) of this order.
  - (3) Chairs the ESC.

- (4) Establishes and provides direction and oversight to ITP multi-organizational or multi-functional groups in accordance with Section 3.a.(1) of this order, including:
  - (a) The ITPWG to assist the DSO in developing, coordinating and operating the ITP; and
  - (b) A single centralized insider threat Analysis and Referral Center (ARC) to collect, integrate, review, assess and initiate referrals or appropriate responses based on information from intelligence, counterintelligence, security, information technology, information assurance, human capital, law enforcement and other sources as necessary and appropriate.
- (5) Individually, or through DSO delegation to another individual or group:
  - (a) Ensures the ITP is consistent with the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, other national directives and DOE requirements;
  - (b) Ensures policies and procedures are developed and maintained for the ITP in accordance with the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, other national directives and DOE requirements;
  - (c) Ensures the ITP is developed and operated in accordance with all applicable privacy, civil liberty and whistleblower protection requirements;
  - (d) Ensures insider threat response actions (investigation, enforcement, etc.) are appropriately documented and completed for ITP purposes;
  - (e) Integrates all elements of the ITP into an operational capability, which includes resolving conflicts between competing interests;
  - (f) Ensures policies, procedures and agreements are established to enable appropriate and timely sharing of information, programs and systems to implement and operate the ITP;
  - (g) Ensures ITP policies and procedures include protecting and appropriately limiting access to analysis procedures, data and results to authorized personnel as required to perform their functions;
  - (h) Establishes and maintains ITP training and awareness requirements for all DOE employees and contractors;

- (i) Ensures personnel assigned to the ITP are fully trained in applicable areas;
  - (j) Ensures that ITP-generated records and applicable System(s) of Records(s) are developed, maintained, protected and shared by Federal and contractors employees as required;
  - (k) Facilitates and coordinates oversight reviews of the ITP;
  - (l) Establishes procedures for insider threat response actions to clarify or resolve insider threat matters;
  - (m) Establishes a user monitoring capability on classified networks and systems; and
  - (n) Ensures program personnel have authorized access to insider threat-related information and data from DOE Elements and other agencies.
- (6) Provides resource recommendations to the Secretary of Energy.
  - (7) Ensures that an annual ITP progress/status report is provided to the Secretary of Energy.
  - (8) Ensures that DOE submits quarterly reports on Key Information Sharing and Safeguarding Indicators (KISSI) to the SISSSC.
- c. Executive Steering Committee (ESC).
- (1) Advises the DSO regarding management, direction, guidance and oversight of the ITP.
  - (2) Includes senior management representation from, at a minimum, the Office of Intelligence and Counterintelligence, Office of Environment, Health, Safety and Security, Office of the Chief Information Officer, Office of the Chief Human Capital Officer, Office of the General Counsel and NNSA.
  - (3) Addresses resource needs of the ITP.
  - (4) Reviews and concurs with or rejects the annual ITP progress/status report to the Secretary of Energy.
  - (5) Designates members of the ITPWG from nominations of sponsoring offices.

- d. ITP Working Group.
  - (1) Includes representation as designated by the ESC, including senior staff level representation from, at a minimum, the Office of Intelligence and Counterintelligence, Office of Environment, Health, Safety and Security, Office of the Chief Information Officer, Office of the Chief Human Capital Officer, Office of the General Counsel and NNSA.
  - (2) Supports the DSO by:
    - (a) Reviewing implementation of ITP policies and procedures and advising the DSO as to program status;
    - (b) Recommending actions and resources to improve the ITP; and
    - (c) Drafting the annual report and providing it to the ESC for review.
  - (3) Provides a forum to address cross-organizational issues.
  - (4) Provides other support and recommendations to the DSO as needed.
- e. DOE ITP Analysis and Referral Center (ARC).
  - (1) Develops and documents DSO-approved insider threat detection, assessment and referral criteria and procedures.
  - (2) Identifies and documents data sources and format(s) needed to support the ARC's designed analytic operations.
  - (3) Gathers, integrates and analyzes information derived from counterintelligence, security, information assurance, human capital, law enforcement, the monitoring of user activity and other sources as necessary and appropriate to identify potential insider threat activity for referral and response.
  - (4) Develops DSO-approved policies and procedures for protecting and appropriately limiting access to ARC analysis procedures, data and results to authorized personnel as required to perform their functions.
  - (5) Through the DSO or according to DSO-approved procedures, refers identified and potential insider threat issues to the appropriate program(s) or office(s) that should lead investigation(s) or other response(s).
  - (6) Recommends to the DSO which DOE or other agencies' program(s) or office(s) should be notified for each identified/potential insider threat.
  - (7) Requests support from other DOE/NNSA elements as needed to develop recommendations for insider threat response and mitigation actions.

- (8) Develops a method(s) to maintain information about all referrals that are performed by the ARC to enable review of ARC analytics performance and to support future searches of historical ARC referrals.

f. Local Insider Threat Working Groups (LITWG).

- (1) Develop and maintain a collaborative environment to identify, coordinate, and integrate local activities to address insider threats.
- (2) Maintain awareness of all factors affecting the risk from insider threats.
- (3) Facilitate access to local data to support the DOE ARC's analytic responsibilities.
- (4) Coordinate activities to assist local authorities, as assigned by a program office or NNSA, to ensure that local insider threat data and records are developed, maintained, shared and protected as required.

g. DOE General Counsel.

- (1) Provides legal advice and assistance to support development and operation of the ITP as required.
- (2) Provides legal advice to the DSO, ESC, ITPWG and ARC.

h. Office of Intelligence and Counterintelligence.

- (1) Reviews, analyzes and assesses ITP data for indications of counterintelligence concerns.
- (2) Participates in the ESC, ITPWG and the ARC.
- (3) Establishes and provides guidance to and develops DSO-approved requirements for LITWGs.
- (4) Provides funding and technical resources to support ITP collection and analysis activities.
- (5) Provides facilities for the ARC.

i. Office of Environment, Health, Safety and Security.

- (1) Coordinates with the ITP to provide and receive security-related information.
- (2) Reviews insider threat indicators for security relevance.
- (3) Participates in the ESC, ITPWG and ARC.

- (4) Provides funding and technical resources to support ITP security concerns.

j. Office of the Chief Information Officer.

- (1) Facilitates ITP data collection and user monitoring needs regarding information networks, technology and systems.
- (2) Ensures that all ITP laws, regulations and policies regarding information system user notification, acceptable use, acknowledgement, training and awareness are satisfied.
- (3) Participates in the ESC, ITPWG and ARC.
- (4) Provides funding and technical resources to support ITP activities.
- (5) Advises the DSO, ITPWG and ARC regarding ITP record creation, management and retention requirements.

k. Office of the Chief Human Capital Officer.

- (1) Ensures identification of and access to appropriate data sources to support the needs of the ITP, including, but not limited to, personnel files, travel records and disciplinary files.
- (2) Applies and advises the ESC, DSO, ITPWG and ARC regarding pre-employment screening tools and procedures that may be used to identify and eliminate insider threats.
- (3) Ensures that new employee briefings include ITP requirements, rights and responsibilities.
- (4) Participates in the ESC, ITPWG and ARC.
- (5) Provides funding and technical resources to support ITP activities.
- (6) Recommends potential sanctions against Federal employee(s) based on human capital procedures.

l. DOE Program and Staff Offices.

- (1) Ensure that planning, data, technical, training, analysis, fiscal and other support to the ITP throughout their organizations is provided as needed.
- (2) Ensure that all employees are aware of individual and organizational ITP requirements and responsibilities.

- (3) Ensure that employee legal, civil and privacy rights are preserved and protected.
- (4) Provide direction to all contractors regarding ITP requirements and responsibilities in accordance with applicable contract requirements.
- (5) Ensure that employees report insider threats consistent with the provisions of the ITP.
- (6) Notify contracting officers of affected contracts that must include the CRD.
- (7) Ensure that local insider threat data and records are developed, maintained, shared and protected as required.

m. National Nuclear Security Administration.

- (1) Ensures that planning, data, technical, training, analysis, fiscal and other support to the ITP throughout NNSA is provided as needed.
- (2) Ensures that all NNSA employees are aware of individual and organizational ITP requirements and responsibilities as applicable to NNSA elements.
- (3) Ensures that NNSA employee legal, civil and privacy rights are preserved and protected.
- (4) Provides direction to all NNSA contractors regarding ITP requirements and responsibilities in accordance with applicable contract requirements.
- (5) Ensures that NNSA employees report insider threats consistent with the provisions of the ITP.
- (6) Notifies NNSA contracting officers of affected NNSA contracts that must include the CRD.
- (7) Ensures that local insider threat data and records are developed, maintained, shared and protected as required.
- (8) Participates in the ESC, ITPWG and ARC as required.

n. Contracting Officers.

- (1) Upon notification by a DOE/NNSA line management official initiating a procurement activity, incorporate ITP CRD(s), requirements or clauses into affected contracts as appropriate.

6. REFERENCES.

- a. Executive Order (E.O.) 10450, Security Requirements for Government Employment, dated April 27, 1953, as amended.
- b. E.O. 12333, United States Intelligence Activities, as amended by Executive Orders 13284 (2003), 13355 (2004), and 13470 (2008).
- c. E.O. 12829, National Industrial Security Program, dated January 6, 1993.
- d. E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, dated June 30, 2008.
- e. E.O. 13526, Classified National Security Information, dated December 29, 2009.
- f. E.O. 13556, Controlled Unclassified Information, dated November 4, 2010.
- g. E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, dated October 7, 2011.
- h. Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, dated November 12, 2012.
- i. White House Memorandum on Early Detection of Espionage and Other Intelligence Activities through Identification and Referral of Anomalies, dated August 23, 1996.
- j. White House Memorandum on Compliance with President's Insider Threat Policy, dated July 19, 2013.
- k. Presidential Decision Direction/NSCC-12, Security Awareness and Reporting of Foreign Contacts, dated August 5, 1993.
- l. Privacy Act of 1974, as amended.
- m. Secretary of Energy Memorandum, Establishment of a Department of Energy Insider Threat Program, dated December 9, 2013.
- n. 10 CFR Part 1045, Nuclear Classification and Declassification.
- o. 32 CFR Part 2001, Classified National Security Information.
- p. DOE O 206.1, *Department of Energy Privacy Program*, dated January 16, 2009.



- q. DOE O 452.7, *Protection of Use Control Vulnerabilities and Designs*, dated May 14, 2010.
- r. DOE O 452.8, *Control of Nuclear Weapon Data*, dated July 21, 2011.
- s. DOE O 457.1A, *Nuclear Counterterrorism*, dated August 26, 2013.
- t. DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated March 1, 2010.
- u. DOE M 471.3, Admin Chng 1, *Manual for Identifying and Protecting Official Use Only Information*, January 13, 2011.
- v. DOE Order 471.3, Admin Chng 1, *Identifying and Protecting Official Use Only Information*, dated January 13, 2011.
- w. DOE O 471.6 Administrative Change 1, *Information Security*, dated November 23, 2012.
- x. DOE 475.1, *Counterintelligence Program*, dated December 10, 2004.
- y. DOE O 475.2A, *Identifying Classified Information*, dated February 1, 2011.
- z. Intelligence Authorization Act for Fiscal Year 1995.

## 7. DEFINITIONS.

- a. “Cleared Employee” means an employee who has been properly granted access to classified information.
- b. “Employee” is defined, for the purposes of this Order, according to the definition in the National Insider Threat Policy; specifically, a person, other than the President and Vice President, employed by, detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.
- c. “Insider” means any person with authorized access to any government or contractor resource to include personnel, facilities, information, equipment, networks or systems.
- d. “Insider Threat” means the threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of classified information, or through the loss or

degradation of U.S. Government resources or capabilities. “Insider Threat Response Action(s)” means activities conducted to ascertain whether certain matters or information indicates the presence of an insider threat, as well as activities to mitigate the threat. Such an inquiry or investigation can be conducted under the auspices of Counterintelligence, Security, Law Enforcement, or Inspector General elements depending on statutory authority and internal policies governing the conduct of such in DOE.

8. CONTACT. For information about this Order, contact the Office of Environment, Health, Safety and Security at (301) 903-4642.

BY ORDER OF THE SECRETARY OF ENERGY:



DANIEL B. PONEMAN  
Deputy Secretary



## **ATTACHMENT 1. CONTRACTOR REQUIREMENTS DOCUMENT**

Regardless of the performer of the work, the contractors must comply with the requirements of this contractor requirements document and with National Nuclear Security Administration (NNSA) and other Department of Energy (DOE) program office direction approved by the DOE Insider Threat Program Executive Steering Committee and provided through contract. Each contractor is responsible for disseminating the requirements and NNSA or other DOE program office direction to subcontractors at any tier to the extent necessary to ensure the contractor's and subcontractor's compliance with the requirements.

Contractors must provide data, information, systems, and any other support to the DOE Insider Threat Program in accordance with applicable laws, regulations, policies, directives and other requirements as directed through contract by the NNSA or other DOE program office(s).

A violation of the provisions of the contract/CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection of section 234B of the Atomic Energy Act of 1954, as amended (42 U.S.C. § 2282b). The procedures for the assessment of civil penalties are set forth in 10 CFR Part 824, *Procedural Rules of the Assessment of Civil Penalties for Classified Information Security Violations*.



## Department of Energy

Washington, DC 20585

November 16, 2014

### MEMORANDUM FOR HEADS OF DEPARTMENTAL ELEMENTS, LABORATORY DIRECTORS, AND FIELD AND SITE OFFICES

FROM:

ERNEST J. MONIZ  
SECRETARY OF ENERGY

ELIZABETH SHERWOOD-RANDALL  
DEPUTY SECRETARY OF ENERGY

SUBJECT:

Laboratory Memoranda of Understanding, Work for Others, Cooperative Research and Development Agreements, and Agreements for Commercializing Technology with Foreign Partners

This memorandum sets forth policies and procedures governing pre-negotiation Headquarters review of all Memoranda of Understanding (MOUs),<sup>1</sup> as well as statements of work for Work for Others (WFO) and Cooperative Research and Development Agreements (CRADAs), between DOE National Laboratories and any foreign partner whether governmental or private.<sup>2</sup> These procedures also apply to Headquarters review of statements of work proposed at DOE laboratories under Agreements for Commercializing Technology (ACT) involving foreign entities. Effective immediately, this memorandum supersedes the Secretary of Energy's memorandum of May 14, 2012, entitled "Laboratory Memoranda of Understanding (MOUs) with Foreign Partners."

Any MOU between a DOE National Laboratory and a foreign partner must meet three tests. The MOU must:

- Align with the strategic interests and policies of the United States
- Be legally sound
- Address any counterintelligence considerations

To ensure that MOUs with foreign partners meet these tests, the May 14 memorandum required pre-signature review of MOUs by the Senior Counterintelligence Officer for the laboratory and DOE Site Office counsel. The memorandum further required submission of signed MOUs to the Headquarters Office of International Cooperative Activities (IA-31) within the (now renamed) Office of International Affairs. Those requirements continue to apply under this memorandum.

Headquarters review should not impede valuable cooperation between laboratories and foreign partners. We have determined, however, that Headquarters review, including by the Office of

<sup>1</sup>"MOU" includes Memorandum of Understanding, Statement of Intent, Letter of Intent, Declaration of Principles, or similar document, whatever its title, between a DOE lab and a foreign partner.

<sup>2</sup> Foreign partner includes a foreign government ministry or agency, foreign laboratory, foreign research institute, international organization, or other entity in a foreign country, as well as any individual who is a citizen or national of a foreign country. MOUs may not be entered into with individuals.



International Cooperative Activities, the Office of Intelligence and Counterintelligence, and the Office of the General Counsel, should be conducted prior to negotiation of laboratory MOUs.<sup>3</sup> Such pre-negotiation review will better ensure that all laboratory MOUs meet the three tests described above. The same concerns – consistency with the strategic interests and foreign policy of the United States, legal soundness, and counterintelligence considerations – also warrant Headquarters review of proposals for WFO, CRADAs, and ACT with foreign partners.

As described in further detail below, IA-31 shall be the point of contact for Headquarters review of laboratories' proposed engagements with foreign partners, and shall coordinate that review with relevant Headquarters offices, including the cognizant Program Office.<sup>4</sup> Proposed laboratory MOUs should be sent to IA-31 and the cognizant Headquarters Program Office upon completion of review by the Senior Counterintelligence Officer for the laboratory and DOE Site Office counsel. To ensure proper Headquarters routing, laboratories in their review requests should identify to IA-31 the technologies and associated Headquarters Program Office with equities in that technology.

Proposed statements of work/proposals for WFO, CRADAs, and ACT with foreign partners should be transmitted to IA-31 and the cognizant Headquarters Program Office in accordance with current procedures. To ensure proper Headquarters routing, laboratories should identify to IA-31 the Headquarters offices (if any) that have already cleared the proposal. All Headquarters reviews will be completed within 10 business days following confirmation of receipt. Headquarters approval will be the responsibility of the Secretary or his designee, and IA-31 will coordinate with the Secretary or his designee as appropriate.<sup>5</sup>

The absence of a response from IA-31 to the laboratory within the 10 business day period shall be deemed consent for the laboratory to (a) negotiate and sign the MOU,<sup>6</sup> (b) draft, negotiate, and execute the WFO agreement or CRADA in accordance with the procedures prescribed in the respective governing DOE Order, or (c) draft, negotiate, and execute the ACT transaction in accordance with governing authorities for ACT. Issues identified by Headquarters reviewing offices and communicated to the laboratory within the 10 business day period must be satisfactorily resolved before negotiation and signature of the MOU, or proceeding with a WFO agreement, CRADA, or ACT transaction, will be authorized. These time frames will ensure that Headquarters review does not delay or impede valuable international collaboration.<sup>7</sup>

---

<sup>3</sup> Prior to negotiation means before tabling or discussing the draft text of a proposed MOU.

<sup>4</sup> "Cognizant Program Office" means both the DOE HQ Program Office that oversees the laboratory's M&O contract as well as the DOE HQ Program Office(s) whose technology(ies) are involved in the foreign engagement.

<sup>5</sup> IA-1 or IA-30 is the Secretary's designee for all non-NNSA laboratories. Pursuant to section 3202 of the NNSA Act, the Deputy Secretary will be the Secretary's designee with respect to draft MOUs, and WFO, CRADA, and ACT proposals between the three NNSA weapons laboratories and foreign entities.

<sup>6</sup> The exception is if the MOU is to be signed in a foreign language in addition to English. See Section I.B for procedures relating to signature of MOUs in foreign languages.

<sup>7</sup> Headquarters approval or consent pursuant to this memorandum does not obviate the need for other approvals that are required under other applicable DOE authorities.

## I. Laboratory MOUs

Laboratory MOUs with foreign partners may be utilized exclusively to memorialize the signatories' intention to conduct informal, non-R&D collaboration, such as exchanging publicly available information on jointly decided subject matters, holding meetings and workshops, and expressing the intent to engage in visits and assignments of personnel to each other's facilities and/or transfer equipment, samples, and materials. A MOU may be utilized as a framework to plan for the future conduct of collaborative R&D by the DOE lab and a foreign partner, but the actual conduct of such R&D can only be under a legally binding contractual instrument such as a WFO agreement (*see* Section II below) or CRADA (*see* Section III below), under the ACT program (*see* Section IV below), or under a legally binding international agreement to which the United States Government or DOE is the U.S. signatory party and which is coordinated through the relevant Headquarters Program Office.

As stated above, pre-negotiation review of proposed laboratory MOUs with foreign partners will be conducted by IA-31, which will coordinate with the Secretary or his designee and with relevant Headquarters offices, including the Office of Intelligence and Counterintelligence and the Office of the General Counsel. Approval to negotiate and sign the MOU shall be the responsibility of the Secretary or his designee. IA-31 will communicate to the laboratory point of contact approval or disapproval for the laboratory to negotiate and sign the MOU. Substantive departures from the approved MOU text must be reviewed by DOE Site Office Counsel before the MOU may be signed; changes in the identity of the foreign partner(s) must be reviewed by the laboratory's Senior Counterintelligence Officer.

The following principles provide guidance concerning conclusion of MOUs between DOE laboratories and foreign partners. When submitting a request for review, laboratories must state how the proposed MOU aligns with these principles by filling out the questionnaire attached to this memorandum and including it with their submission.

1. In the long-term, there must be an affirmative benefit to DOE and/or the U.S. Government from the partnership.
2. The partnership must be consistent with the foreign policy and national security interests and priorities of the U.S. Government.
3. Work under the MOU must comply with all applicable U.S. Government policies and DOE procedures.
4. Work under any proposed MOU must be consistent with the long-term goals and objectives of DOE and the relevant DOE programs must be notified.
5. The collaboration should not create a resource burden on a DOE Program Office or DOE Laboratory.
6. The partnership should aim to leverage domestic capabilities to advance U.S. scientific achievement or clean energy technologies and potentially enhance the Department's or Laboratory's stature and global leadership.

7. The partnership should aim to advance global efforts in areas related to the DOE mission including, for example, environmental protection and remediation, energy security, reducing greenhouse gas emissions, or nuclear security and nonproliferation.
8. The partnership should aim to provide a benefit to the U.S. economy through lower cost technologies for consumers, export markets for domestic companies, U.S. based jobs, or similar economic advantages.

These principles should also be considered in developing proposals for WFO, CRADAs, and ACT with foreign partners, but submission of the attached questionnaire is required only for proposed MOUs.

#### *A. Assistance in Drafting MOUs*

IA-31 has developed, and provided to the laboratories, guidance on the proper drafting of MOUs with foreign partners; and the relevant country desk officer within IA-31 can advise on whether a proposed MOU aligns with U.S. strategic interests and policies, provide general information on the bilateral relationship between the United States and the country of the foreign partner, and provide other assistance concerning preparation of informal MOUs. In addition, IA-31 has developed the COMmitment Management International Tracking (COMMIT) database to archive the Department's international commitments, including MOUs. Labs can contact [labagreements@hq.doe.gov](mailto:labagreements@hq.doe.gov) to request copies of existing MOUs and agreements with foreign partners. Labs can also access existing DOE MOUs directly through IA's website ([www.energy.gov/ia/icc-documents](http://www.energy.gov/ia/icc-documents)); the database only contains lab MOUs completed since May 2012. Legal questions may be addressed to the Assistant General Counsel for International and National Security Programs within the Office of the General Counsel at 202-586-3417.

#### *B. Signing a MOU in a Foreign Language in Addition to English*

If a foreign partner desires to sign a MOU in its own language, in addition to English, the laboratory should obtain a draft of the foreign language text from the foreign partner after mutual agreement on the English language text has been reached, and send both the English and foreign language texts to the Office of International Cooperative Activities. IA-31 will coordinate review of the conformance of the English and foreign language texts by the Department of State's Office of Language Services, which charges non-commercial rates for this service. The laboratory will be responsible for paying these charges. IA-31 will handle arrangements to receive the required funds from the laboratory and transfer them to the State Department for performance of the dual language conformance review.

Language conformance can add considerably to the time required to prepare a MOU for signature. No laboratory may sign a MOU in a foreign language until the Department of State's Office of Language Services has confirmed to IA-31 in writing that the English and foreign language texts are in conformance with each other.<sup>8</sup>

---

<sup>8</sup> Language conformance ensures that the MOU text has the same substantive meaning in both languages; it does not concern or address stylistic matters such as orthographical conventions (e.g., program vs programme, or recognize vs recognise).



## II. Work for Others (WFO)

DOE Order 481.1C, *Work for Others (Non-Department of Energy Funded Work)*, governs the conduct of work for non-DOE entities by DOE (including NNSA), as well as the use of DOE/NNSA facilities that is not directly funded by DOE appropriations. The Order authorizes DOE laboratories to conduct work funded directly by foreign sponsors, with the following requirements:

- "Work directly funded by a foreign sponsor and performed at a non-NNSA facility requires the review and concurrence of the [IA Office of International Cooperative Activities] and the cognizant program office." (Section 4.1.)
- "Work directly funded by a foreign sponsor and performed at an NNSA facility requires the review and concurrence of the NNSA Office of Institutional and Joint Programs." (Section 4.m.)<sup>9</sup>

The responsibilities of other DOE and NNSA elements with respect to review and approval of WFO contracts are addressed in Sections 5 and 6, respectively, of Order 481.1C and in DOE Manual 481.1-1A (*Reimbursable Work for Non-Federal Sponsors Process Manual*).

In addition to these requirements, effective immediately, we direct that all technical proposals/statements of work for proposed WFO agreements where the work is directly funded by a foreign sponsor shall be reviewed by Headquarters, with IA-31 acting as the central point of contact. Site Offices or laboratories (in accordance with local procedure) shall submit the technical proposal/statement of work to IA-31 and the relevant Headquarters Program Office. IA-31 will coordinate Headquarters review by the relevant office(s), which review will be completed within 10 business days following receipt of the WFO proposal. The absence of a response from IA-31 within this 10 business day period shall be deemed consent for the laboratory to proceed with drafting and negotiating the WFO agreement in accordance with the procedures set forth in DOE Order 481.1C and Manual 481.1-1A. Issues identified by Headquarters reviewing offices and communicated to the laboratory within the 10 business day period must be satisfactorily resolved before the laboratory may proceed with negotiating and executing the WFO agreement.

## III. Cooperative Research and Development Agreements (CRADAs)

DOE labs are authorized to enter into CRADAs by statute (15 U.S.C. 3710a) and regulation (48 CFR 970.5227-3). DOE Order 483.1A, *DOE Cooperative Research and Development Agreements*, sets forth DOE policy, requirements, and responsibilities for the oversight, management, and administration of CRADA activities at DOE facilities. With respect to

---

<sup>9</sup> DOE O 481.1C and DOE M 481.1-1A utilize, but do not define, the term "foreign sponsor", although the Order, in Section 8.1., defines "non-DOE entities" to include "international organizations; and foreign governments." For purposes of this memorandum, "foreign sponsor" with respect to WFO means any entity over which control is exercised or exercisable by a foreign national, foreign government, or foreign entity. "Foreign entity" means any branch, partnership, group or sub-group, association, estate, trust, corporation or division of a corporation organized under the laws of a foreign state and whose principal place of business is outside the United States.

CRADAs with foreign participants, section 3710a(c)(4)(B) directs that "[t]he laboratory director in deciding what [CRADAs] to enter into, shall . . . in the case of any industrial organization or other person subject to the control of a foreign company or government, as appropriate, take into consideration whether or not such foreign government permits United States agencies, organizations, or other persons to enter into [CRADAs] and licensing agreements."<sup>10</sup> Also, a FOCI (Foreign Ownership, Control or Influence) certification is required for agreements concerning the transfer of technology involving participant access to classified information, special nuclear materials, or unescorted access to security areas of Departmental facilities.<sup>11</sup>

In addition to the foregoing requirements, effective immediately, we direct that all proposals for CRADAs with foreign participants shall be reviewed at Headquarters, with IA-31 acting as the point of contact. Site Offices or laboratories (in accordance with local procedure) shall submit a summary of the work under a proposed CRADA to IA-31 and the cognizant Headquarters Program Office. IA-31 will coordinate Headquarters review by the relevant office(s), which review will be completed within 10 business days following receipt of the CRADA proposal. The absence of a response from IA-31 within this 10 business day period shall be deemed consent for the laboratory to proceed with drafting and negotiating the CRADA in accordance with the procedures set forth in DOE O 483.1A. Issues identified by Headquarters reviewing offices and communicated to the laboratory within the 10 business day period must be satisfactorily resolved before the laboratory may proceed with negotiating and executing the CRADA.

#### IV. Agreements for Commercializing Technology (ACT)

Under the authority of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.), DOE initiated a pilot program in 2012 entitled Agreements for Commercializing Technology. ACT provides DOE's M&O contractors with another mechanism to conduct third-party sponsored research in furtherance of the Department's technology transfer mission. In exchange for privately assuming certain risks and liabilities normally borne by private sponsors, M&O contractors are authorized to negotiate ACT agreements using terms that may be more consistent with comparable private sector agreements.

Under ACT, the participating laboratories may conduct research for non-federal entities where such work does not interfere with work the contractor conducts on behalf of the government. The work also must comply with Federally Funded Research and Development Centers' (FFRDC) requirements applicable to the facility, and must be performed in accordance with the applicable M&O contract clause (the ACT "H Clause") enabling ACT activities at the facility. The ACT H Clause requires contractors to perform all ACT activities in accordance with the standards, policies, and procedures that apply to performance under its M&O contract (including

---

<sup>10</sup> DOE O 483.1A references, but does not define, "foreign participant". For purposes of this memorandum, "foreign participant" with respect to CRADAs means any entity over which control is exercised or exercisable by a foreign national, foreign government, or foreign entity. "Foreign entity" means any branch, partnership, group or sub-group, association, estate, trust, corporation or division of a corporation organized under the laws of a foreign state and whose principal place of business is outside the United States.

<sup>11</sup> The FOCI review and certification will be performed by the Headquarters FOCI coordinator in the Office of Health, Safety and Security, in consultation with the Office of the General Counsel.

security and counterintelligence procedures); to specifically identify any foreign ownership or control of ACT agreement parties; and to include additional information, as necessary or requested by the Contracting Officer, whenever an ACT agreement includes a foreign entity.<sup>12</sup>

In addition to these requirements, effective immediately, we direct that all technical proposals/statements of work for proposed ACT transactions involving foreign entities shall be reviewed at Headquarters prior to any approval or determination by the cognizant Contracting Officer.<sup>13</sup> ACT technical proposals/statements of work and requests should be transmitted to IA-31 and the cognizant Headquarters Program Office. IA-31 will coordinate review by relevant Headquarters offices, which review will be completed within 10 business days following receipt of the ACT proposal. The absence of a response from IA-31 within this 10 business day period shall be deemed consent for the Contracting Officer to make the requisite approval or determination. Issues identified by Headquarters reviewing offices and communicated to the laboratory within the 10 business day period must be satisfactorily resolved before the approval or determination will be authorized.

#### V. Points of Contact

IA-31 will be the central point of contact for coordinating the DOE Headquarters review of proposed MOUs and WFO, CRADA, and ACT proposals described in this memorandum. The email address for all submissions is [labagreements@hq.doe.gov](mailto:labagreements@hq.doe.gov). Each laboratory should provide to IA-31, within 10 business days of the date of this memorandum, the name and other contact information for its point(s) of contact with IA-31. A laboratory may, if desired, designate different points of contact for MOUs, WFO, CRADAs, and ACT.

Laboratories shall send a pdf copy of each final, fully executed MOU with a foreign entity to IA-31 at [labagreements@hq.doe.gov](mailto:labagreements@hq.doe.gov) within 20 business days of signature.

Attachment:

- Laboratory MOU Questionnaire

---

<sup>12</sup> This memorandum applies to ACT transactions with any entity over which control is exercised or exercisable by a foreign national, foreign government, or foreign entity. Foreign entity means any branch, partnership, group or subgroup, association, estate, trust, corporation or division of a corporation organized under the laws of a foreign state and whose principal place of business is outside the United States.

<sup>13</sup> Under the model ACT H Clause, section 4di, contractors may request a "preliminary determination" that proposed work is consistent with the facility mission. If the preliminary determination finds that the work is consistent with the mission, the contractor may begin conducting the work pending a final decision on the complete approval package. Preliminary determinations are designed to accommodate sponsors that need work done on a more expedited schedule.

## LABORATORY MOU QUESTIONNAIRE

1. In the long-term, is there an affirmative benefit to DOE and/or the U.S. Government from the partnership?
2. Is the partnership consistent with the foreign policy and national security interests and priorities of the U.S. Government?
3. Does the work under the MOU comply with all applicable U.S. Government policies and DOE procedures? If not, please explain.
4. Is the work under the MOU consistent with the long-term goals and objectives of DOE and will the relevant DOE programs be notified of activity undertaken through the MOU? If not, please explain.
5. Does the collaboration create a resource burden on a DOE Program Office or DOE Laboratory?
6. Does the partnership aim to leverage domestic capabilities to advance U.S. science and technology related to DOE's missions in science, energy, nuclear security, and environmental protection and remediation, and potentially enhance the Department or Laboratory's stature and global leadership?
7. How does the partnership aim to advance global efforts in areas related to the DOE missions?
8. How does the partnership aim to provide a benefit to the U.S. economy?