CNS | consolidated nuclear security, llc

# Security Requirements for Registered Non-Possessing Facilities

This summarizes the safeguards and security responsibilities of:

with its principal office and place of business at:

doing business covered by this plan at the following location(s):

## Non-Possessing Facility Subcontract Requirements

The provisions of our contract with the Department of Energy (DOE) and/or with a DOE contractor do not authorize our company to receive, store, transmit, or originate classified information within our facility(ies). However, performance of work under this contract will require at least some of our personnel to hold DOE access authorizations for access to classified information and/or special nuclear material (SNM) at other approved DOE facilities. We understand that our company is responsible for ensuring that all personnel involved in this contract — including company managers, employees, and direct consultants, as well as any lower-tier subcontractors whose employees require DOE access authorizations — comply with all applicable DOE security requirements, including the following:

SELLER personnel responsible for safeguarding, handling, possessing, or processing Unclassified Controlled Nuclear Information (UNCI) Legacy Official Use Only (OUO) information, or Controlled Unclassified Information (CUI) must first successfully complete the Information Protection briefing/training provided by the CNS Classification Office, CUI Program Office (Y-12 865-241-4995), or designee. SELLER's lower-tier subcontractors and/or suppliers are also required to complete the same requisite briefing/training by the CNS Classification Office prior to being provided access to UCNI, Legacy OUO or CUI. The SELLER shall be responsible for coordinating any additional personnel for briefing/training. The SELLER will provide the CNS Classification Office, CUI Program Office, with briefing/training records of all individuals trained including lower-tier subcontractors and/or suppliers. The SELLER shall be responsible for the control of all UCNI, Legacy OUO and CUI documents and media and is not relieved of this obligation for documents provided to others. The Information Protection briefing/training is required to be administered biennially (i.e., within 24 months) SELLER must maintain current training records for all SELLER personnel responsible for safeguarding, handling, possessing, or processing UCNI, Legacy OUO or CUI. Additional briefing/training or instructions may be directed by the BUYER at the BUYER's discretion.

**Security Training [DOE O 470.1A]**

- *Arranging for the Facility Security Officer (FSO) to complete training as necessary to implement all of the requirements in this plan, as well as other applicable provisions of the underlying DOE directives.*
- *Identifying any other company and subcontractor personnel who assist the FSO in implementing this plan — e.g., access authorizations — and arranging for training as necessary to ensure compliance with DOE requirements.*
- *The SMO must appoint the FSO and Insider Threat Program Senior Official (TPSO) in writing. The SMO, FSO, ITPSO and Key Management Personnel roles can be held by the same person.*
- *FSO and ITPSO training must be completed within 6 months of appointment to the position.*

# Security Requirements for Registered Non-Possessing Facilities

**Access Authorizations [DOE O 472.2A. 1, Att. 1]**

- *Obtaining access authorizations as soon as possible for all Key Management Personnel (KMPs) identified in the Foreign Ownership, Control or Influence (FOCI) determination at the same level as the company's facility clearance.*
- *Obtaining other access authorizations only as required to perform work involving access to classified information and/or SNM, and only at the level required by each individual.*
- *Handling and submitting all access authorization requests and maintaining personal clearance-related documentation about individuals in accordance with the Privacy Act of 1974.*
- *Maintaining current information about all active access authorizations, including each cleared individual's name, DOE file number, date of clearance notification, and the classified contract(s) for which an access authorization is held.*
- *Ensuring that cleared individuals are aware of their responsibility to directly notify DOE of potentially relevant information — e.g., arrests, bankruptcies, garnishments, name changes, marriage/cohabitation, etc.*
- *Notifying DOE within two working days after the company becomes aware of a cleared individual's mental health treatment or any other condition that might cause a significant defect in judgment or reliability.*
- *Notifying DOE through established channels as soon as possible — but no later than two working days— when an individual no longer requires an access authorization (e.g., termination of employment or transfer to unclassified work).*

**Security Briefings [DOE O 470.4C]**

- *Ensuring that all company and subcontractor personnel — regardless of clearance status — receive initial security briefings prior to being allowed unescorted access to any DOE security area(s) under the company's control.*
- *Ensuring that all cleared company and subcontractor personnel receive comprehensive security briefings and execute SF-312, Classified Information Nondisclosure Agreement, before receiving access to classified information.*
- *Ensuring that all cleared company and subcontractor personnel receive annual security refresher briefings within the time frames prescribed by the DOE or prime contractor's Security Awareness Coordinator.*
- *Ensuring that cleared company and subcontractor personnel receive security termination briefings and complete DOE F 5631.29, Security Termination Statement, when their DOE access authorizations are terminated.*
- *Maintaining records of initial, comprehensive, refresher, and termination security briefings in a manner that the dates on which company and subcontractor personnel received these briefings.*

**Security Badges [DOE O 473.1A, Att. 2, Chapter XI]**

- *Ensuring that all company and subcontractor personnel who are granted access authorizations also receive standard DOE photo badges.*
- *Ensuring that any visitor, temporary, and/or other local site-specific (LSSO) badges used by the company comply with DOE requirements, including restrictions relating to foreign nationals.*
- *Ensuring that all individuals who receive a DOE security badge are aware of the requirement to report lost or stolen badges to the issuing Badge Office within 24 hours.*
- *Recovering DOE security badges as soon as company and subcontractor personnel terminate or otherwise no longer require badges, and immediately returning them to the issuing Badge Office.*

**Official Travel [DOE O 550.1, Chg. 1]**

- *Ensuring that all company and subcontractor personnel who engage in official foreign travel comply with all pre-trip notification and briefing requirements established by the sponsoring DOE or contractor organization.*
- *Ensuring that all company and subcontractor personnel who engage in official foreign travel submit post-travel trip reports within 60 days after returning to their duty stations.*

# Security Requirements for Registered Non-Possessing Facilities

**Facility Clearance [DOE O 470.1A**

- *Protecting all Government property in the company's possession and submitting a property control security plan to DOE for approval if the company becomes responsible for more than $5 million in Government property.*
- *Ensuring that any solicitations for lower-tier contracts or other agreements with other companies that require their personnel to obtain access authorizations contain the notice at DEAR 952.204.72, Facility Clearance.*
- *Submitting a DOE F 470.1, Contract Security Classification Specification (CSCS), through appropriate channels and obtaining DOE approval before awarding a lower-tier agreement that requires access authorizations to another company.*
- *Ensuring that any lower-tier agreements awarded to other companies that will require access authorizations contain the clauses at DEAR 952.204-2, Security, and DEAR 952.204-70, Classification/Declassification.*
- *Submitting a CSCS form to DOE through appropriate channels if significant changes occur in a previously registered agreement — e.g., the extension of the contract end date or the termination of work requiring access authorizations.*

**FOCI [DOE O 470.1A]**

- *Notifying DOE immediately of any actual or anticipated changes in FOCI that might affect the company's current FOCI status — e.g., a change from "No" to "Yes" in an item on SF-328, Certificate Pertaining to Foreign Interests.*
- *Providing to DOE if any changes have occurred in the company's ownership; its officers, directors, and executive personnel; or the information in the company's last full FOCI certification.*

**Classification Guidance [DOE O 475.2B]**

- *Ensuring that any company personnel certified as Derivative Classifiers (DCs) or UCNI Reviewing Officials (RO) for work at other facilities receive all required training, including Classified Matter Protection and Control (CMPC) requirements..*
- *Ensuring that any company personnel whose work involves generating matter at other facilities that might be classified receive CMPC training and are aware of the procedures for obtaining DC/RO reviews.*
- *Any issues relating to classification should be referred to the Field or Program Classification Officer for advice and assistance.*

**Incidents of Security Concern [DOE O 470.1A, Att 6.]**

- *Ensuring that all company personnel who are authorized access to classified information and/or SNM at other facilities are aware of the requirements and procedures for immediately reporting security infractions or incidents.*
- *Establishing an incident management program that provides for appropriate disciplinary measures if DOE determines that company personnel have committed security infractions or incidents.*
- *Any Incidents of Security Concern (IOSC) should be reported to the appointed IOSC Program Manager.*

**Survey Reviews [DOE O 470.4C]**

- *Reviewing the company's compliance with DOE requirements in implementing the applicable security programs covered by plan must be conducted at intervals not to exceed every 36 months.*
- *Documenting the results of these self-assessments; preparing corrective action plans for any deficiencies; and tracking corrective actions until fully implemented.*

# Security Requirements for Registered Non-Possessing Facilities

| | |
|---|---|
| **Personally Identifiable Information (PII) [DOE O 206.1, Chg. 1 Att. 1]** | • *Ensure that actions are taken to address data breaches of PII that is collected, processed or maintained on paper records, stored and/or transmitted through DOE computer systems, and sensitive data owned by DOE that is properly stored on non-DOE computer systems.* |
| **Unclassified Controlled Nuclear Information (UCNI) [DOE O 471.1B]** | • *Ensures that matter identified as UCNI is protected in accordance with the instructions contained in DOE O 471.1B and 10 CFR 1017, Identification and Protection of Unclassified Controlled Nuclear Information Subpart E – Physical Protection Requirements.*<br>• *Ensure data containing UCNI remains access controlled on CNS authorized computing devices and all applicable electronic storage and sharing practices comply with CNS guidance.*<br>• *Ensure that access to documents marked as containing UCNI is only provided to those individuals authorized for routine access per 10 CFR 1017 and who need to know the information to perform their jobs or other DOE-authorized activities.*<br>• *Reports any incidents involving the unauthorized disclosure of UCNI, Legacy OUO, or CUI to the Y-12 Operations Center at 865-574-7172.* |
| **Controlled Unclassified Information [DOE O 471.7, Admin. Chg. 1]** | • *Ensure that documents determined to contain Legacy OUO information are marked and protected as described in DOE O 471.7, Legacy Information Waiver, and DOE policies.*<br>• *Ensure that documents that contain CUI are accessed only by properly trained and authorized personnel.*<br>• *Ensure data containing CUI remains access controlled on CNS authorized computing devices and all applicable electronic storage and sharing practices comply with CNS guidance.*<br>• *Ensure that access to (a) documents marked as containing CUI is only provided to those persons who need to know the information to perform their jobs or other DOE-authorized activities.*<br>• *Reports any incidents involving the unauthorized disclosure of CUI to the Y-12 Operations Center at 865-574-7172.* |
| **Insider Threat Program [DOE O 470.5A]** | • *Regardless of the performer of the work, the contractors must comply with the requirements of the Contractor Requirements Document (CRD) 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.*<br>• *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).*<br>• *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.* |
| **Other Undertakings [Specify]** | • |

# Security Requirements for Registered Non-Possessing Facilities

Our company will develop internal procedures as needed to implement all applicable DOE security requirements and inform company and subcontractor personnel of their individual responsibilities for implementing these requirements. In addition, company and subcontractor personnel will comply with applicable security procedures at the sites where work involving classified information and/or SNM is performed.

Our company understands that, at least every five years, designated DOE representatives must inspect our facilities compliance with all applicable DOE safeguards and security requirements. Upon request, company personnel will provide DOE with documentation for these reviews. If DOE notifies our company in writing that its security procedures and/or practices do not comply with DOE security requirements, we will submit an appropriate corrective action plan to DOE within 30 working days and provide at least quarterly progress reports until DOE determines that all deficiencies are corrected.

**CERTIFICATIONS**

As the designated Facility Security Officer, I accept lead responsibility for ensuring company compliance with all applicable DOE security requirements.

_____ Typed Name _____ Signature

_____ Telephone Number _____ Date

_____ E-Mail

The undersigned management representative certifies that the Facility Security Officer has been given the authority, resources, and other management support needed to ensure company compliance with all applicable DOE security requirements. If a new Facility Security Officer is appointed, the company also agrees to immediately notify DOE and to execute a new UCN-20856, and provide to the CNS, LLC Procurement Representative.

_____ Typed Name _____ Signature

_____ Official Title _____ Date