# Sandia National Laboratories (SNL) Specific Safety and Security Requirements

# SOFTWARE, SERVICES & INFORMATION SYSTEMS SECURITY ASSURANCE

1. Subcontractor warrants that all items, information systems, software and services, including cloud-based service models (e.g., infrastructure as a service, platform as a service, or software as a service) provided under this subcontract are free of code or other mechanisms that: collect personal information, assert control of the system without NTESS’ consent, or which may restrict NTESS’ access to or use of company data. Subcontractor further warrants that it will not knowingly introduce, via any means, spyware, adware, ransomware, rootkit, keylogger, virus, trojan, worm, or other code or mechanism designed to permit unauthorized access to the NTESS data, or which may restrict NTESS access to, or use of NTESS data or compromise NTESS data.
2. Subcontractor shall use due diligence to verify that features, functions, and capabilities of deliverables conform to specifications. Subcontractor represents that deliverables only contain features and/or functions that are disclosed.
3. If Subcontractor suspects or becomes aware of any threat events, security incidents, or vulnerabilities in Subcontractor’s operations, products, and/or services, Subcontractor shall provide written notice to contractnotification@sandia.gov within 48 hours.
4. Subcontractor shall cooperate fully with NTESS to investigate all potential security incidents, threat events, and/or vulnerabilities.

# NOTE: As used in this clause, the terms “threat event” and “vulnerability” have the meanings defined in NIST SP 800-30. The term “security incident” has the meaning defined in NIST SP 800-53. Security incidents include, but are not limited to: malfunctions due to design/implementation errors and omissions, targeted malicious attacks, untargeted malicious attacks, insider threats, unintended capabilities, and compromises/breaches involving information system components, information technology products, and development processes or personnel.

# DISCLOSING USE OF FREE, LIBRE AND OPEN SOURCE SOFTWARE (FLOSS) AND THIRD-PARTY SOFTWARE (TPS)

*This clause applies to subcontracts that include the delivery of software (including software residing on hardware).*

Subcontractor shall disclose in writing any FLOSS and/or TPS delivered in connection with this subcontract. Send written disclosures to the SP listed on this first page of this subcontract and contractnotification@sandia.gov.

1. FLOSS refers to software that incorporates, embeds, uses, bundles, or otherwise associates with any of the following:
	1. Open source, publicly available, or "free" software, library or documentation
	2. Software licensed under a FLOSS License
	3. Software provided under a license that subjects the delivered software to any FLOSS License, or requires the delivered software to be licensed for the purpose of making derivative works or be redistributable at no charge
2. FLOSS License(s) include any Free Software, Open Source and Public License(s). FLOSS License also refers to: General Public License (GPL), Lesser/Library GPL (LGPL), the Affero GPL (APL), the Apache license, the Berkeley Software Distribution (“BSD”) license, the MIT license, the Artistic License (e.g., PERL), the Mozilla Public License (MPL), or variations thereof.

**SOFTWARE ASSURANCE DOCUMENTATION - 291SA (04-18)**

In accordance with Section II clauses DISCLOSING USE OF FREE, LIBRE AND OPEN SOURCE SOFTWARE (FLOSS) and SOFTWARE, SERVICES & INFORMATION SYSTEMS SECURITY ASSURANCE, Subcontractor shall include with applicable deliverables:

1. Identification of FLOSS content in any deliverable, which has been pre-approved by the Subcontracting Professional in writing,

2. Documentation which discloses all features and/or functions of software,

3. Notification of any threat events, security incidents, or vulnerabilities that may have the potential to affect the functionality, security, or integrity of software, services or information systems.

**QUALITY ASSURANCE PROGRAM - 108QAP (10-18)**

The Subcontractor's Quality Assurance (QA) program shall control activities that may affect the quality of the item(s) or service(s) specified in the contract, Statement of Work (SOW), or documents incorporated by reference. Subcontractor's QA program shall meet or exceed requirements in 10 CFR 830 and DOE O 414.1 (latest version applicable at the date of this subcontract) (https://www.directives.doe.gov/; examples of compliance include ISO9001, AS9100, ASME NQA-1) and be documented via written policies, procedures, or instructions. Subcontractor shall adhere to its QA program during performance of this subcontract.

**SAFEGUARDING HANDLING AND TRANSMISSION OF INFORMATION - 633DST (05-17)**

All drawings, specifications, technical information, subcontract or proposal-related information, project management information, and lower tier supplier information supplied to the Subcontractor or generated by the Subcontractor shall be protected from unauthorized use, reproduction, and disclosure and Subcontractor shall protect the information at least to the same extent it would use to protect its own most valuable and proprietary information. Dissemination or use of such information is limited to such of its employees and Subcontractors, if any, whose job performance for this specific subcontract

requires the information and only for those purposes. No other dissemination or use is permitted without prior written approval of the Subcontracting Professional/Sandia Delegated Representative.

All electronic information transmitted by the Subcontractor shall be protected with appropriate levels of encryption or Transport Layer Security (TLS).

**LOWER TIER SUPPLY CHAIN – 142LSC (10-18)**

Subcontractor agrees that all subcomponents, software, services, and deliverables pertaining to this work are domestically sourced, and that information pertaining to Subcontractor work for NTESS is restricted from exposure to lower tier subcontractors or suppliers.

**NON-US CORPORATE AFFILIATES – 140NCA (10-18)**

Information and deliverables pertaining to this specific subcontract work or NTESS shall not be shared or disclosed with any non-US affiliates such as parent, child, or associate branch companies.

**NON-US LABOR DISCLOSURE – 141NLD (10-18)**

Subcontractor shall disclose to the Subcontracting Professional whether information or deliverables pertaining to this subcontract work or NTESS will be shared or disclosed with any non-US citizen who may be performing work at Subcontractor site.

**PERSONAL IDENTITY VERIFICATION FOR EXTENDED PHYSICAL AND CYBER ACCESS – 600ACC (10-19)**

In accordance with NNSA SD 206.2, *Implementation of Personal Identity Verification (PIV) for Uncleared Contractors*, background investigations may be required for uncleared subcontractor and lower-tier subcontractor employee(s) requiring physical or cyber access to NTESS/SNL or DOE/NNSA owned or leased facilities and/or designated Information Technology (IT) systems for more than 179 calendar days. This includes any physical and cyber access combinations that exceed 179 days.

The Subcontractor will be notified by SNL Personnel Security when the uncleared Personal Identity Verification (PIV) background investigation process is required. The Subcontractor shall ensure eligible employee(s) and lower-tier Subcontractor employees comply with the PIV process which includes:

A. Electronic fingerprinting,

B. Two forms of identification and having a photo taken, and

C. Completion of SF85, Questionnaire for Non-Sensitive Positions and OF306, Declaration for Federal Employment*.*

Unfavorable PIV determinations will result in immediate revocation of physical and/or cyber access, and may result in the Subcontractor and lower-tier Subcontractor employee(s) removal from performance of work under this agreement. Uncleared Subcontractor and lower-tier Subcontractor employee(s) may appeal unfavorable PIV determinations to DOE/NNSA.

Compliance with PIV procedures is required for Subcontractor and lower-tier Subcontractor employee(s) continued authorization to perform work and access to NTESS/SNL and DOE/NNSA sites and IT systems.

For any additional questions, contact SNL Security Connection at (505) 845-1321 or security@sandia.gov.

RESOURCES

FSO Toolcart (https://www.sandia.gov/FSO/index.htm), NTESS resource for badging, access, and security information.

**HOMELAND SECURITY - 600HLS (10-19)**

Performance of this subcontract requires physical access to facilities owned or leased by NTESS and/or Department of Energy/National Nuclear Security Administration (DOE/NNSA).

A. The Subcontractor shall ensure employees' and lower-tier Subcontractor employees' compliance with NTESS/DOE/NNSA procedures for obtaining physical access and provide accurate information on forms submitted.

B. The Subcontractor shall affirmatively disclose its participation and any employee participation in any Foreign Government Talent Recruitment Programs (FGTRP- as defined in DOE Order 486.1).

1. The Subcontractor and any lower-tier Subcontractor shall notify NTESS within seventy-two (72) hours if it, or any of its employees are, or are reasonably believed to be, participants in a foreign government talent recruitment

program(s) during performance of this subcontract. Notifications to ContractNotification@sandia.gov.

2. The Subcontractor shall include this clause in its entirety, in any subcontract at any tiers awarded in the performance of this subcontract, in which employee(s) of the subcontractor will require physical access to NTESS

and/or DOE/NNSA owned or leased facilities.

3. Upon NTESS direction, Subcontractor agrees to remove employee(s) participating in any FGPT from work under

this Agreement.

C. Subcontractor shall return the badge(s) or other credential(s) provided by NTESS or DOE/NNSA pursuant to this clause, granting physical access to DOE/NNSA-owned or leased facilities by Subcontractor's employee(s), upon:

1. The termination of this subcontract

2. The expiration of this subcontract

3. The removal of an individual performing work under this subcontract or any subcontractor employees performing

work under this subcontract; or

4. NTESS or DOE/NNSA direction.

RESOURCE(S)

FSO Toolcart (https://www.sandia.gov/FSO/index.htm), NTESS resource for badging, access, and security information.

**SUBCONTRACT SPECIFIC SAFETY - 603CSS (09-17)**

In performing the work under this subcontract, Subcontractor shall perform work safely, in a manner that ensures adequate protection for employees, the public, and the environment, and shall be accountable for the safe performance of work in accordance with DEAR 970.5223-1, Integration of Environment, Safety, and Health (ES&H) Into Work Planning and Execution. NTESS is required to flow these requirements to the Subcontractors at any tier.

This requirement operates in addition to any other specifications or requirements included elsewhere in this subcontract. The Subcontractor shall flow down these requirements to all applicable lower-tier subcontractors. All work on electrical systems shall require the Subcontractor to provide evidence (training, certifications, licensing) that the Subcontractor employees performing the electrical work are qualified.

If an injury or accident occurs during the performance of this work on a Department of Energy/National Nuclear Security Administration (DOE/NNSA) site, the Subcontractor shall verbally report the incident as soon and as safely as possible. **For emergencies**, at Sandia National Laboratories/New Mexico (SNL/NM), call 911 or from mobile phone (505) 845-0911/(505)

844-0911/(505) 284-0911; and, at Sandia National Laboratories/California (SNL/CA), call 911 or from mobile phone (925) 294-2222. **For non-emergencies**, at SNL/NM, call 311 or from mobile phone (505) 845-0311/(505) 844-0311/(505) 284-0311; and, at SNL/CA, call 311 or from mobile phone (505) 844-0311. **Notify the Sandia Delegated Representative (SDR) after this reporting is complete.**

NTESS' FULL SET REQUIREMENT

For work performed on a DOE/NNSA site, the Subcontractor and its employees shall comply with NTESS' full set of Corporate Policy System requirements in the ES&H Policy Area, as well as any additional site specific safety requirements (training, permitting, Work Planning and Controls). The Subcontractor and its employees shall not begin work on a DOE/NNSA site until a Pre-Job Briefing, including authorization for work to begin, has been provided by the SDR.

Declaration of Occupational Medicine Provider

Subcontractors that meet the applicability criteria below shall establish and provide comprehensive occupational medicine services to workers employed at DOE-controlled premises, in accordance with 10 CFR 851, Worker Safety and Health Program. Subcontractors that will perform any work on a DOE site, and that meet the applicability criteria below, shall provide the SDR a written declaration by completing form SF 4040-DOP, located at http://www.sandia.gov/resources/employees/corporate\_forms/, identifying its Occupational Medicine Provider, as applicable. The declaration must be completed and provided to the SDR prior to performing work. The declaration is maintained with the project files. The Subcontractor shall maintain a copy of the completed declaration.

Applicability Criteria:

1. Work on a DOE site for more than thirty (30) days in a 12-month period

OR

2. Are enrolled for any length of time in a medical or exposure monitoring program required by this rule and/or any other applicable Federal, State or local regulation, or other obligation.

# ENVIRONMENTAL, SAFETY, AND HEALTH (ES&H) REQUIREMENTS

1. Service Providers - NTESS-directed work. NTESS shall provide those workers with any and all necessary safety authorization documents, personal protective equipment, industrial hygiene monitoring, medical surveillance, and radiation protection services.
2. Service Providers - Subcontractor-directed work. Subcontractor shall provide its workers with all ES&H services, with the exception of Subcontractor employees performing Subcontractor-directed work on government sites for whom NTESS shall provide radiation dosimetry services and survey of record, as appropriate.
3. Training Requirements. Any Subcontractor personnel who will enter a government site to perform work shall have completed all of the ES&H training required by the SOW prior to any attempts to enter a government site as shown by written records of such training furnished to the SDR or to the Requester if no SDR is named in Section I of this subcontract. Subcontractor shall certify to NTESS completion of all required training on the Completion Record for Subcontractor Administered Training form. This form is located on the Web at <http://www.sandia.gov/working_with_sandia/current_suppliers/contract_information/index.html> under the “Forms” tab, or obtained from the SDR. Subcontractor shall provide the completion record form for the initial ESH100 training to the SDR on the first day of work. Subcontractor shall provide the completion records for any other training required above to the SDR before starting the affected work activity. Any person not having completed all ES&H training requirements may be denied access to any government site and Subcontractor may be terminated for default of this subcontract as well as every other subcontract the Subcontractor has with NTESS.

**SUB****CONTRACTOR, LOWER-TIER SUBCONTRACTOR, AND VISITOR ACCESS REQUIREMENTS**

1. Government-Controlled and Government-Owned sites. The Subcontractor agrees and shall ensure that Subcontractor and lower-tier subcontractor personnel entering government-controlled and government-owned sites for any activity related to this subcontract shall at all times be subject to and shall comply with all laws, regulations, policies, and site access rules for the site including, but not limited, to all ES&H and Security requirements. For work performed at government-controlled and government-owned sites, the Security and ES&H requirements can be obtained by contacting the SDR. The government requirements include, but are not limited to, those set forth in this clause for any work to be performed on a government-controlled or government-owned site.
	1. To obtain access to government-controlled or government-owned site, the Subcontractor shall submit an email request to the SDR or SP stating the company designation to be used by the Subcontractor and each lower-tier subcontractor and furnishing the following information on each Subcontractor and lower-tier subcontractor personnel requiring access to the government-controlled and government-owned site:
		1. Name
		2. Date of birth
		3. Citizenship status
		4. Completed ES&H training requirements set forth in the SOW of this subcontract
	2. Access will be granted for the period of performance as stated in Section I of this subcontract.
	3. Subcontractor shall withdraw and replace any Subcontractor or lower-tier subcontractor personnel, assigned to perform work under this subcontract, who in the judgment of NTESS or DOE/NNSA, is to be denied access to any government-controlled or government-owned site.
	4. Subcontractor shall submit to the SDR any proposed working schedules for its personnel and that of each lower-tier subcontractor that deviate from NTESS' normal workday or work week schedule as noted in Section I of this subcontract. The schedules shall show proposed daily working hours and proposed work weeks. Schedules that deviate from NTESS' normal work day or work week must be approved by the SDR.
	5. In the absence of a written authorization from the SP or SDR, use of government-controlled or government-owned sites by the Subcontractor and its lower-tier subcontractors, pursuant to access granted under this clause, shall be limited to work as set forth in the SOW of this subcontract to be performed on government-controlled or government-owned.
	6. THE USE OF THE ACCESS PRIVILEGE FOR ANY PURPOSE OTHER THAN TO PERFORM WORK AS SET FORTH IN THE SOW OF THIS SUBCONTRACT IS PROHIBITED AND MAY BE GROUNDS FOR TERMINATING THIS SUBCONTRACT FOR DEFAULT OR DENYING ACCESS TO ANY SUBCONTRACTOR OR LOWER-TIER SUBCONTRACTOR PERSONNEL.
2. SNL Site Access. The organizations listed below are responsible for coordinating and administering the provisions of visitor access and control for the sites as listed.
	1. Sandia National Laboratories, Albuquerque, New Mexico – Badge Office, NTESS, Innovation Parkway Office Complex (IPOC).
	2. Sandia National Laboratories, Livermore, California - Visitor Control and Administration Section, NTESS, Building 911.
	3. Tonopah Test Range, Tonopah, Nevada - Office of the Tonopah Test Range Manager.
3. Subcontractor shall ensure that its and its lower-tier subcontractor personnel assigned to work on government-controlled or government-owned sites comply with all applicable site access requirements. In addition, the Subcontractor and its lower-tier subcontractor personnel, shall:
	1. Not bring weapons of any kind onto government-controlled or government-owned sites
	2. Not manufacture, sell, distribute, possess, use or be under the influence of controlled substances or alcoholic beverages while on government-controlled or government-owned
	3. Not possess hazardous materials of any kind on government-controlled or government-owned sites without SP or SDR authorization or as stated in the SOW of this subcontract
	4. Not venture into unauthorized/restricted areas
4. All persons, property, and vehicles entering or leaving government-controlled or government-owned sites are subject to search by site Security Policy Officers.

**DEFENSE BIOMETRIC IDENTIFICATION SYSTEM (DBIDS) REGISTRATION FOR SUBCONTRACTORS - 601DB (10-19)**

All personnel requiring unescorted access to Kirtland Air Force Base (KAFB) must be registered in DBIDS.

A. If an individual is Q or L cleared and possesses a Homeland Security Presidential Directive-12 (HSPD-12) badge (has a gold chip), the individual must simply visit a DBIDS station listed below and register the badge in the DBIDS system.

B. If the individual is uncleared or does not possess an HSPD-12 badge, a DBIDS pass is required. DBIDS requests require a sponsor to initiate the request and serve as the point-of-contact to notify when passes are available for pick-up. The sponsor must possess an HSPD-12 badge registered in DBIDS. The sponsor should be the company’s Facility Security Officer or a cleared person within the company. If there is no one withing the company is capable of sponsoring the individual, contact the

Sandia Delegated Representative (SDR) for assistance.

C. The type of DBIDS pass depends on the length of unescorted access requested.

1. Short-term pass - For access of 10 days or less, a short-term pass may be immediately issued at a DBIDS station, provided a sponsor is present in person with the applicant. Note that multiple short-term passes are allowed only up to a cumulative of 30 days over a three-month period per year. Beyond that, a long-term pass must be requested.

2. Long-term pass - For access up to one year, a long-term pass is necessary requiring submission of the following documentation:

a. Criminal Background Check Form SF 2730-CBC

b. Visitor Pass Request Form SF 2730-VPR

c. A typed letter of justification that contains

(i) The reason for the request

(ii) Dates and times of the needed access

(iii) Location to which the individual needs access

(iv) Duration of the pass

(v) Signature of the person sponsoring the individual for access

This documentation must be submitted in person (i.e., not emailed or faxed) to a DBIDS station by the listed sponsor. The sponsor will be notified when the long-term pass is available for the applicant to pick up. Ten days are required to process a long-term pass. In the interim, a short-term pass may be issued at the time of application.

D. When notified by the sponsor, the individual shall go to a DBIDS Station to pick up their long-term DBIDS pass. The individual must have an NTESS badge with them when they pick up their DBIDS card; otherwise, the DBIDS sponsor will need to be present. When obtaining any DBIDS pass, the individual must provide photo identification compliant with the REAL ID Act (e.g., compliant state-issued driver’s license/ID card, U.S. passport, military ID, etc.). Failure to do so will result in denial of access. Visit http://ttr.sandia.gov/forms/acceptableformsofidentification.pdf for a list of acceptable forms of

photo identification. The identification documents must be in original form (not copies), unaltered, unexpired, and valid (not cancelled or suspended).

DBIDS Stations:

1. Pass and Registration Section in the Consolidated Support Building located at Building 20245

2. Truman Gate Visitors Center, which is minimally manned and may require additional time

3. Innovation Parkway Office Center (IPOC) Building

For any additional questions, please contact the KAFB Pass and Registration Office at 505-846-6429 or your SDR.