VISITOR GROUP SECURITY AGREEMENT (VGSA)
ADDENDUM TO DD FORM 254

Per 32 CFR, Part 117, National Industrial Security Program (NISP): Industrial Security (IS) Procedures for Government Activities, contractor's personnel assigned to a United States Government (USG) controlled installation to perform operations that require access to classified information for the Commander or a Government Contracting Activity, are considered visitors and are subject to the security procedures of the installation. The baseline requirements follow; however, there are procedures that are unique to the specific host installation, and references for each are provided herein. The following agreement sets forth the security requirements for contractor personnel who maintain an operational presence at Strategic Systems Programs (SSP) Headquarters or any of its field activities:

1. This agreement, by and between SWFLANT (hereinafter referred to as host activity) and _____ (hereinafter referred to as "Contractor Visitor Group"), prescribes specific security requirements to be carried out by Contractor Visitor Group personnel assigned to a Host Activity. This agreement is consistent with the requirements set forth in the NISP: IS Procedures for Government Activities. The NISP IS procedures stipulate the requirements for Contractor Operations on a United States Government (USG) Controlled Installation. The purpose of this agreement is to ensure the protection of Government-owned National Security Information (NSI) entrusted to the Contractor Visitor Group performing duties at the host activity. The provisions of this agreement also apply to subcontractors performing under this contract. Responsibilities are delineated as follows:

a. ***Authority.*** The Commander or designee will provide security oversight of all Contractor Visitor Groups. As such, Contractor Visitor Group will comply with the security procedures of the host activity specific to this contract.

b. ***All Parties.*** All parties will comply with the provisions of this agreement without exception or deviation. The Command / Activity Security Manager (CSM) is responsible for the implementation, oversight, and management of the Industrial Security Program for the host activity.

c. ***Contractor Security Supervision.*** The Contractor Visitor Group's Home Office Facility (HOF) will designate, in writing, the names of primary and alternate security representatives responsible for security administration at both their cleared facility and at the host activity operating location. The host activity CSM is responsible for providing oversight and is responsible for implementing and managing the government activity security program.

d. ***Standard Practice Procedures (SPP).*** Compliance with this agreement obviates the need for the Contractor Visitor Group to have an addendum or supplement to the HOF SPP that would outline security responsibilities at the host activity. The Contractor Visitor Group will comply with the host activity's security procedures; security procedures identified in this VGSA take precedent over the contractor's SPP.
Should Contractor Visitor Group personnel determine a need to develop an addendum or supplement to the HOF SPP, a copy must be provided to the host activity CSM.

e. ***Access to and Accountability of Classified Material***

(1) Access to NSI by the Contractor Visitor Group will be under the control of the host activity and will be granted on a need-to-know basis. Contractor Visitor Group will not have custody of NSI, however, an individual from the group is permitted to be nominated as a Classified Control Representative (CCR), in order to ensure safekeeping of classified information at the host activity. NSI will be returned to a host activity employee for appropriate storage or disposition when no longer in use by Contractor Visitor Group.

(2) Should Contractor Visitor Group, during contract performance, discover unattended classified material or an unsecure/unattended security container, they will immediately secure the classified material and notify a host activity on-site employee, as well as the Contractor's Security Office, and host activity CSM. During non-duty hours, Contractor Visitor Group will notify the host activity CSM, who will then notify the Command Duty Officer (CDO) of a potential loss or compromise of NSI. Contractor Visitor Group will maintain and have on-hand a list of emergency telephone numbers should there be a need to reach any of the aforementioned points of contact. NSI will be released to the CDO should the CCR be unavailable.

f. ***Storing of Classified Material*:** Classified material for use by Contractor Visitor Group will be issued by host activity personnel, and will be stored in a government certified open storage area or in a classified storage container, or both. Contractor Visitor Group is not authorized to permanently store classified material at the host activity.

g. ***Transmitting Classified Material:***

(1) Contractor Visitor Group is not authorized direct receipt or dispatch of NSI at the host activity location. For postal receipt, Contractor Visitor Group will use the following address:

Host Activity:	Address:
SWFLANT	Commanding Officer, SWFLANT, 1150 USS Los Angeles Road, Kings Bay, GA 31547-2637, Attn: Document Control

(2) NSI to be transmitted by U.S. postal channels directly from host activity must be prepared and processed through the classified information control system of the host activity location. Select applicable reference here SWFLANT M-5530.7 (Series).

(3) Classified material may be hand carried locally within the Area of Responsibility (AOR) by Contractor Visitor Group via a DD Form 2501, *Courier Authorization Card.* Follow reference SWFLANT M-5530.7 (Series) to brief document courier on hand carrying procedures.

h. ***Disposing Classified Material.*** When NSI is no longer needed or when the contract performance ends, Contractor Visitor Group will return any and all NSI that was provided to or created by them, to the host activity CSM. Any other methods of disposition must be coordinated with the on-site CSM.

i. ***Reproducing Classified Material.*** Only government approved reproduction equipment will be used to reproduce classified materials. Contractor Visitor Group is not authorized to copy classified material without prior approval from the host activity CSM.

j. ***Security Education.*** Contractor Facility Security Officer (FSO)/Local Security Representative must brief Contractor Visitor Group on their responsibility for safeguarding classified information. Contractor Visitor Group will be briefed on a recurring, but not less than annual basis. The briefing may be tailored only to those responsibilities associated with their assigned duties.

k. ***Personnel Security Clearances (PCLs).*** The FSO will ensure all DoD PCL eligibility and access information for the Contractor Visitor Group is verified through the approved DoD system of record for PCLs. The FSO is responsible for initiating and tracking security eligibility investigations for Contractor Visitor Group personnel who will have access to classified information, as required by DD Form 254.

(1) FSO is responsible for submitting a Visit Access Request (VAR) for the Contractor Visitor Group through the approved DoD personnel system of record for PCLs. VARs will be submitted annually to the applicable host activity's Security Management Office (SMO) Code: 68733 SWFLANT.

(2) The host activity CSM will "Service" Contractor Visitor Group PCLs in the approved DoD system of record for PCLs.

(3) When a member of the Contractor Visitor Group is no longer required to be on-site at host activity, they will be required to be debriefed, and the debriefing will be recorded on OPNAV 5511/14, *Security Termination Statement*. OPNAV 5511/14 will be maintained by the host activity CSM and destroyed when no longer needed.

l. ***Reports.*** As referenced in block 13 of DD254, contractor must submit to the host activity CSM, in writing, any and all security violations committed by Contractor Visitor Group. Reports must be submitted within 24 hours of any incident(s).

(1) The commanding officer of the host activity initiates Preliminary Inquiries (PI). Appointed officials coordinate inquiry/investigation reports with the host activity CSM.

(2) Contractor Visitor Group will advise host activity CSM of any changes in their operations that could affect operations at the host activity; these changes include changes in management, personnel, location, or contractual performance.

m. ***Access and Restricted Area Badges)***. Access to a host activity requires the Contractor Visitor Group to obtain a host activity-specific government picture badge and, when applicable, a Common Access Card (CAC). Procedures for obtaining government badges are dependent on host activity requirements.

Contractor Visitor Group will follow procedures for their specific host activity (e.g., SPHQ, SWFLANT, SWFPAC, PMOSSP Pittsfield).

(1) Badging procedures for host activity locations are as follows:

SWFLANT:
Access to SUBASE requires Contractor Visitor Group to obtain a Defense Biometrics Identification System (DBIDS) credential. When required for contract performance, either a locally produced SUBASE Restricted Area Access Badge, SWFLANT Limited Area (LA) badge, or both, will be issued to Contractor Visitor Group for entry into SUBASE Restricted Areas.

SUBASE Restricted Area Access Badge: When required for contract performance, Contractor Security or COR (if on-base) will submit a SUBASE badge application and SWFLANT LA badge application to CSM. Contractor security representative or COR will specify area accesses required on the application for employees as required for their job performance. CSM will process the application and notify contractor security representative when complete. Requests for access will be supported by visit request, security eligibility verification, and need-to-know.

(2) CAC. A CAC is only authorized for personnel who require logical access to a government network (.mil email address). The FSO or COR will request a CAC for employees through the host activity CSM, utilizing the Trusted Associate Sponsorship System (TASS). The contractor security representative will submit a TASS Registration Request (TRR) to the government sponsor who will validate the need for a CAC. The government sponsor will forward the TRR to the host activity's Trusted Agent (TA) for processing. The continued need for the CAC will be verified semi-annually by the government sponsor, TA, and FSO. The CAC will be turned in to the TA upon contract termination, loss of employment, or when there is no longer a continued need for a CAC. CACs are valid for up to 3 years or for the length of the contract, whichever comes first. Expired CACs require a new TRR.

(3) FSO/Local Security Representative is responsible for ensuring that Contractor Visitor Group is briefed on the proper wear of issued badges while on duty at host activity. Refusal or repeated neglect to display the issued badges may result in the unsuitable determination per reference SWFLANT M-5530.7 (Series). Upon termination or resignation, or any other event leading to a Contractor Visitor Group employee leaving duty under this contract, the contractor is responsible for returning all Government identification, building passes and other government property issued to that employee.

(4) Contractor Visitor Group employees will immediately notify the CAC or badge issuing authority should they lose a CAC or badge.

n. ***Security Checks.*** Contractor Visitor Group will perform security checks within assigned work areas at the host activity. These checks will ensure security precautions are taken to protect NSI issued to the Contractor Visitor Group. Contractor Visitor Group will follow reference SWFLANTINST 5530.7 for end-of-day security checks. Standard Form 701, *Activity Security Checklist,* and Standard Form 702, *Security Container Check sheet,* will be used to record these checks and maintained for 30 days from date of completion or as required.

o. ***Emergency Protection.*** In the event of an emergency (e.g., natural disaster, major accident, security alerts, or civil disturbance), the Contractor Visitor Group will follow the emergency procedures of the host activity. The CSM will brief the Contractor Visitor Group on these procedures prior to performing work at the host activity location.

p. ***Protecting Government Resources.*** Contractor Visitor Group will comply with host activity procedures for protecting government resources, SWFLANTINST 5530.7

q. ***Clarification of Security Requirements.*** Contractor Visitor Group will submit written requests for clarification of security requirements through SWFLANT CSM.

r. ***DD254.*** This agreement is an addendum to DD Form 254, as such, Contractor will maintain a copy of the associated DD Form 254 at the host activity operating location. Government COR will ensure DD Form 254 is current, that revisions are accomplished when required, and biennial reviews are completed.

s. ***Foreign Involvement.*** Under the terms of this agreement, Contractor Visitor Group will notify Host Activity CSM and contracting office, prior to any foreign involvement, regardless of access requirements or the sensitivity of information to be disclosed (classified or unclassified), unless covered under the auspices of the US/UK Polaris Sales Agreement. In addition, visits to the Host Activity, to include foreign national visits, must be processed through and approved by the Host Activity CSM.

2. ***Program Reviews***

a. The Host Activity Industrial Security Specialist will conduct an initial industrial security program review of the Contractor Visitor Group operations upon arrival of the contractor.

b. Subsequent industrial security program reviews will be accomplished per sub paragraphs (1) and (2).

(1) The Host Activity CSM conducts annual program reviews of the Contractor Visitor Group's on-base activity to ensure compliance with this security agreement. A written program review report will be provided to the COR and the FSO. Contractor is not required to acknowledge receipt of the report or respond unless directed to do so.

(2) Host Activity CSM will include the FSO in the annual security self-inspection program. The CSM will use the VGSA requirements and the Command self-inspection criteria to perform the annual self-inspection on the Contractor Visitor Group operations, and to document and maintain the inspection report as required by the procedures outlined in reference SWFLANT M-5530.7.

3. ***Review of this Agreement.*** All parties must review this agreement for accuracy at least annually. Host Activity Industrial Security Specialist is responsible for keeping this agreement current. COR is responsible for the agreement and will maintain a copy of the last program review. In addition, Host

Activity CSM will keep on file for three years, copies of evaluations and self-inspections, or equivalent reviews. Copies of reports will be forwarded to Contractor for their records.

4. ***Communication Security (COMSEC).*** Contractor Visitor Group will use Secure Terminal Equipment (STE) when discussing classified information telephonically. SIPRNET will be used when classified information is to be sent via an automatic information system.

a. SIPRNET accounts are available to Contractor Visitor Group personnel upon request. The need for a SIPRNET account will be verified by the FSO/Local Security Representative, who will then submit a System Access Authorization Request (SAAR) to the Host Activity Help Desk for account creation. The CSM will be notified of all Contractor Visitor Group requests for SIPRNET accounts.

b. Contractor Security Representative and Host Activity CSM will validate that the Contractor Visitor Group employee has the appropriate security eligibility and has completed derivative classification training. CSM will also ensure information on the SAAR is complete and correct and has been signed off by the requestor and supervisor. CSM will verify PCL eligibility and access in DoD's system of record and will document on the SAAR. Contractor Security Representative will sign the SAAR and provide employee a North Atlantic Treaty Organization (NATO) briefing and certificate to be signed by the employee.

5. ***Computer Security (COMPUSEC).*** Information systems (IS) (i.e., computers, word processors, networks and stand-alones, etc.) used in the processing of classified information in support of this contract must be approved prior to commencement of classified operations. Contractor will comply with Host Activity policy for accreditation of information systems used in classified processing.

6. ***Operation Security (OPSEC):***

The Contractor Visitor Group shall:

- Protect critical or sensitive-unclassified operational information.

- Not engage in any illegal or unethical conduct, or any other activity which would constitute a conflict of interest.

- Not reveal or use information received in confidence during a professional assignment, without proper authorization.

- Report all information obtained during the course of an assignment accurately and completely.

7. ***Other Security Programs:*** All Contractor Visitor Group employees and any sub-contractors will be subject to applicable regulations, policies and procedures on Physical Security, Anti-Terrorism/Force Protection (AT/FP) and Law Enforcement.

8. ***Other:***

a. ***Forms.*** COR or CSM furnishes all government forms and Navy Instructions to Contractor Visitor Group as required by this agreement.

b. ***Sub-contracts***. A VGSA will be initiated whenever Contractor enters into a sub-contractual arrangement with another contractor for classified performance at an SSP Host Activity. It must address the sub-contractor's operation separately. The Host Activity Commanding Officer, the CSM, and both Contractor and sub-contractors must sign the agreement. A DD Form 254 is completed for each subcontractor requiring access to classified information. Contractor is responsible for preparing the DD Form 254 and must provide a copy to Host Activity CSM for review to ensure it correctly reflects the instructions furnished by the prime Procuring Contracting Officer (PCO). The PCO must ensure that any questions regarding adequacy of the DD Form 254 are resolved to the mutual satisfaction of Contractor, subcontractor, and the contracting officer, or are referred to the COR for resolution. The prime contractor signs item 17 of the DD Form 254 for subcontracts and makes required distribution.

c. ***Notification.*** Contractor HOF must notify CSM thirty (30) days prior to contract completion/shutdown in order to conduct a review of Contractor operations at Host Activity location to ensure proper disposition of this security agreement, and any classified material entrusted to Contractor Visitor Group personnel.

9. ***Expenditure of Funds for Security.*** The Cognizant Security Office (CSO) (be it DSS or the Commander or head of a USG-controlled installation) will not commit the government to reimburse a contractor for funds expended in connection with the Contractor's security program. In the case of a cost-reimbursement-type contract, the allowability of security costs is determined by the contracting officer in accordance with the terms of the contract and with the cost principles of the Federal Acquisition Regulation (FAR). Under a fixed price contract, the initial contract price includes all applicable security costs. An equitable adjustment may be made in the initial contract prices when, as indicated in the contract security clause, the security classification or security requirements under the contract are changed by the government (e.g., changes to DoD 5220.22-M, and the change results in an increase or decrease in the contract price). DoD 5220.22-M provides that a U.S. contractor must implement changes no later than 6 months from the data of the published change to DoD 5220.22-M to allow the contractor to discuss what impact, if any, the changes have on existing classified contracts.

VISITOR GROUP SECURITY AGREEMENT (VGSA)
ADDENDUM TO DD FORM 254

Agreement accepted by:

_____ _____
(DATE)

Facility Security Officer

_____ _____
(DATE)

Contracting Officer Representative (COR)
Strategic Weapons Facility, Atlantic

_____ _____
(DATE)

Activity / Command Security Manager (CSM)
Strategic Weapons Facility, Atlantic

_____ _____
(DATE)

Commanding Officer
Strategic Weapons Facility, Atlantic