Interconnection Security Agreement
Between
(Name of User Agency)
and
Defense Security Service

References: (a) DODD 8500.1
(b) NISPOM, Chapter 8
(c) (GCA Regulation)

This Interconnection Security Agreement (ISA) between (**User Agency**) and the Defense Security Service (DSS), Designated Approval Authority for (**Company Name**), is for the purpose of establishing a secure communications link between (**User Agency**) and (**Company Name**) for the electronic transfer of classified information. Each of the undersigned agrees to and understands the procedures that will be in effect and adhered to. It is also understood that this ISA summarizes the information system (IS) security requirements for approval purposes and supplements (**Company Name**) approved system security plan (SSP).

1. Contract Information

This ISA describes the classified network arrangement between (**Company Name**) and (**User Agency**) in support of the (**Name of Program**). The (**Name of Program**) is a (**brief description of program**) sponsored by (**User Agency**). The contract number is (**Contract Number**). The Prime contractor is (**Name of Prime Contractor**), whose Cage Code is (**Cage Code Number**).

At (**User Agency**) direction, (**Company or User Agency Name**) is establishing a remote access capability to the (**Name of Classified Computer System and Unique Identifier**); with a remote access IS located at (**List User Agency or Company, as appropriate**). ***(Note to Template User: Please word this paragraph so that it is obvious who will be the host, if applicable, and who will be the remote site(s))***. This capability will allow (**Company or User Agency, as appropriate**) personnel to access the (**List Name of Classified IS and UID**) as remote users. The (**User Agency**) IS is located at (**address**).

The following (DSS) key points of contact are identified:

Name	**Title**	**Phone**	**Email**
Karl Hellmann	NISP Authorizing Official	571-305-6627	Karl.j.hellmann.civ@mail.mil
Jonathan Cofer	DSS HQ MOU Coordinator	571-305-6739	Jonathan.h.cofer2.civ@mail.mil
	Regional Authorizing Official		
	ISSP		

The following (Company) key points of contact are identified:

Name	**Title**	**Phone**	**Email**

The following (User Agency) key points of contact are identified:

Name	Title	Phone	Email

2. Description

(**Company or User Agency Name**) operates the (**List Names of Classified System**) IS at **(Identify C-I-A categorization)**, whereby all users have the clearance and need to know for all information on the system. The highest level of classification of the IS is (**Level of Information**). All personnel with access to the (**Name of Classified System**) will be briefed for (**Give name of specific briefing, e.g. COMSEC**).

(***Describe connection and connection approval process. An example follows***): The (**Company or User Agency Name**) IS will be connected to the (**Name of Classified System at different enclave (if needed)**) at (**Company or User Agency Name at different enclave (if needed)**), by a communication circuit for the transfer of data. The circuit will be protected at each end by an NSA Type 1 encryption device, to provide encryption of the circuit. Operational key for the NSA Type 1 encryption shall be at the **(classification level)** level.

Any further network security requirements not described within this document are detailed in the attached network security plan and connection approval process.

3. Network Information System Security Officer (Network ISSO) Responsibilities

The Network ISSO (**Network ISSO Name**) at (host--**Company and User Agency Name**) will have the following responsibilities. He or she will brief operator personnel involved with use of the communications link on network operating procedures and their responsibilities for safeguarding classified information in accordance with the requirements of paragraph 5-100 of the National Industrial Security Program Operating Manual (NISPOM) or applicable Department of Defense policy. The IS Security Officer at (**List Names of other User Agency or Company Site**) will conduct an equivalent briefing for network responsible personnel.

The Network ISSO at (**Company and User Agency Name**) and the IS Security Officer at (**Name of other site(s)**) will indoctrinate system operators and support personnel concerning:

a. The need for sound security practices for protecting information handled by their respective IS, including all input, storage, and output products.
b. The specific security requirements associated with their respective IS as they relate to need-to-know (NTK) and operator access requirements.
c. The security reporting requirements and procedures in the event of a system malfunction or other security incident occurs.

d. What constitutes an unauthorized action as it relates to system usage.
e. Their responsibility to report any known or suspected security violations.

It is the responsibility of each individual operator to understand and comply with all required procedures for using the **(Name of Classified System at Company Site**), as described in the SSP which is approved by the Defense Security Service (DSS). The system user shall report all instances of any security violations to the ISSM ***(or Network ISSO if located at company)*** at (**Company Name**). In addition, the User Agency IS Security Officer ***(or Network ISSO if located at User Agency)*** will report any security violations to the system.

4. Interconnect Procedures

The communication link at **(Host Site Name)** will be available **(insert hours)** per day. The operating system at the host IS automatically records all operators logging in and out. When logged in, the operators at (**Contractor or User Agency Name**) will be able to access the system for the transfer of classified data.

All signers agree there are no further connections on this network to DISN networks, including the SIPRNet.

Each interconnected site must maintain a current and valid accreditation in accordance with Department of Defense policy.

When the communications link between (**User Agency**) and (**Company Name**) is no longer required, communications between sites will be disabled by removing the remote users from the "system password file" and physically disabling the encrypted link from the router, if applicable. Additionally, the user agency will notify DSS in writing of cancellation of the ISA.

5. Approval

The secure communication link between (**User Agency**) and (**Company Name**) shall not be initialized until approval of these procedures by all AOs is indicated below. This agreement will remain in effect for three years from the date of the signatures below, unless specifically terminated by either AO. This ISA becomes effective upon signatures of all parties.

Defense Security Service	(User Agency)
_____	_____
KARL HELLMANN NISP Authorizing Official	(Name of User Agency Official and Rank) Authorizing Official
Date:	Date: