Remote Link
Classified Information Systems Security Plan (ISSP)

Site Name: _____

Site Address: _____

_____

_____

_____

_____

_____

Date: _____

Introduction

This ISSP uses three "link" terms. The first, the Direct Link, refers to the entire Classified Information System, the link housed at DOE Headquarters (HQ), Germantown, MD and all attached links. The second, the Host Link, refers to all equipment that is located at DOE. The final term, the Remote Link, refers to any stand-alone system of components that is configured for connection to the Host Link.

This ISSP has been developed by the DOE Direct Link Classified Information System Security Officer (IS SO) for a Remote Link connection to the DOE Direct Link in accordance with DOE Manual 471.2-2, Classified Information Systems Security Manual. This ISSP specifically describes the security controls used for safeguarding information being processed, stored, or produced by the Remote Link while operating in an encrypted dial-up session on the Direct Link.

In addition to this Remote Link ISSP being approved in writing by each local Designated Accrediting Authority (DAA), the Remote Link workstation must be accredited for classified processing up to and including Secret-Restricted Data by local authorities and operating at a protection level of one (1). The entire package, as described below, is then forwarded to the Classified Information System Operations Manager (ISOM), DOE Savannah River Operations Office. The DOE Savannah River Operations Office ISOM, who is the network DAA, must review and accredit Remote Links in order to gain access approval to the Direct Link. The entire Remote Link package consists of:

1. Formal letter of request for connection to Direct Link (this may be input prior to submission of package);

2. Accreditation letter by local authority of area where the Remote Link is to be located granting capability to process data up to the Secret-RD level;

3. Full names and other clearance information of individuals requesting access to the Remote Link (this may be provided under the "Operating Environment Information" section of this plan);

4. Locally approved Remote Link ISSP (this appendix completed, or a separate ISSP containing, at a minimum, the information contained in this appendix.).

The final accreditation is the authority for the DOE NMMSS staff to permit access to the system by the Remote Link via an encrypted dial-up link.

The Remote Link ISSP has two attachments, a Security Agreement, Appendix A, and a Security Review Checklist, Appendix B. Both attachments must be completed and accompany this plan when submitted for final accreditation. Upon submittal, please ensure that all sections are complete. Use N/A where the section does not apply. Use additional paper for continuation as necessary. Please type or print all information.

Site Information

Site Name: _____

Site Address: _____

Workstation
Name: _____
Location: _____

Information System Security Officer (IS SO)
Name: _____ Phone: _____
Organization: _____

Communications Security (COMSEC) Officer
Name: _____ Phone: _____
Organization: _____

Information System Security Manager (IS SM)
Name: _____ Phone: _____
Organization: _____

Information Security Operations Manager (ISOM)
Name: _____ Phone: _____
Organization: _____

Local Designated Accrediting Authority (DAA)
Name: _____ Phone: _____
Organization: _____

Remote Link PC Information

Location: _____
Modem Phone No.: _____

Provide a brief description of the Remote Link PC environment.

_____

_____

_____

_____

Note: Please attach design documentation for the Remote Link configuration.

Hardware - List the hardware being used (PC, attached peripherals: printer, STU-III, etc.)

Equipment	Manufacturer	Model #	Serial #
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Software Identification - List the software being used (operating system, telecommunications package, etc.).

Developer	Title	Version No.
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

According to NTISSI 3013, Operational Secure Doctrine for the Secure Telephone Unit III (STU-III) Type 1 Terminal, Annex H, this Remote Link meets the requirements of operating: attended or unattended. (Please circle.)

Estimated Expected Usage: _____ hours per week.

Operating Environment Information

Protection Level: _____

Classification of Information Processed (Enter an "X", where applicable):

		NSI	FRD	RD
Unclassified	Confidential			
	Secret			

Remote Link Operators:

Full Name	Clearance

Remote Link Specific Additions To The
Direct Link Classified Information Systems Security Plan (ISSP)

This section is devoted to the compliance of the Remote Link to the Direct Link ISSP. This section should describe any additional risks or safeguards implemented at the Remote Link that do not appear in the plan. (Enter N/A where no additions exist.)

Security Contracts - Note any security contracts applicable to the Remote Link.

_____
_____
_____

Special Security Countermeasures - Note any special security countermeasures applicable to the Remote Link.

_____
_____
_____

Provide Security Countermeasures - Note any special security countermeasures applicable to the Remote Link.

_____
_____
_____

Site Specific Deviations Form
The Direct Link Classified Information Systems Security Plan (ISSP)

Describe deviations, rationale for non-compliance, and alternate safeguards implemented. Also state applicable reference from Direct Link ISSP. (Enter N/A where no deviations exist.)

Direct Link ISSP Reference: _____

Alternate Procedure: _____

Certification/Accreditation Signatures

Remote Link ISSO Certification:

Name: Signature: Date:_____

Remote Link ISSM Certification:

Name: Signature: Date:_____

Remote Link ISOM Certification:

Name: Signature: Date:_____

Direct Link ISOM/Accrediting Official:

Name:_____ Signature: _____ Date: _____

Appendix A
Security Agreement

Remote Link Name: _____

My signature below certifies that I have read and understand the security procedures contained in this Remote Link Classified Information Systems Security Plan, and I acknowledge, understand, and agree:

To protect any account/password provided to me as Secret - Restricted Data, a level commensurate with the information to which it provides access.

I will not share my account/password with anyone for any reason.

To protect the information accessed or controlled by me at the level indicated by any classification markings or at the level of accreditation of the system.

To use the hardware and software entrusted to me only for official business; that my activities will be monitored for fraud, waste and abuse of the government resources; and that I understand the penalties for such actions.

To introduce no unauthorized software into the processing environment.

To use my access authority appropriately and in the best interest of the U.S. Government; and

To respect the operating rules of the Remote Link.

Printed Name	Signature	Date
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Appendix B
Security Review Checklist

This attachment is used by the Remote Link to provide a method for conducting a security evaluation of the procedures and controls described in the classified ISSP for this Remote Link. Each security area is established as a "test/verification" section containing a series of questions or statements concerning security requirements or safeguards that may be in that specific security area. The ISSO will mark each question with a YES or NO answer as it applies to this Remote Link and, after completing the form, will evaluate the implemented security measures to determine if the Remote Link has been given an adequate protection level of one (1). When satisfied that the security procedures and controls are adequate, the ISSO will sign and date the certification at the end of this attachment and forward all documentation to the ISOM.

_____ All users are cleared for the highest classification level and most restrictive category of information.
_____ The Remote Link is sanitized prior to servicing by uncleared service personnel.
_____ Uncleared maintenance personnel are escorted at all times.
_____ All escorts hold DOE “Q” access authorizations, appropriate need-to-know, and are trained in their responsibilities.
_____ All users read and sign a Security Agreement listing their security responsibilities.
_____ Annual security training is provided to each user and documented.
_____ An authorized and qualified user access list is maintained by the ISSO.
_____ The facility is protected by a security force and only authorized cleared personnel may gain unescorted access.
_____ The Remote Link is located in a Limited Access Area.
_____ Only authorized users have unescorted access to the Remote Link.
_____ The Remote Link is connected to a STU-III data encryption device.
_____ All equipment meets local TEMPEST requirements.
_____ All Red/Black separation criteria have been met.
_____ All media is handled in accordance with local approved accountability procedures.
_____ Removable storage media placed on the system is labeled with the classification level and category at which the Remote Link is accredited.
_____ All hardware is marked with the classification level and category at which the Remote Link is accredited.
_____ Only the ISSO, with the approval of the ISSM, coordinates the relocation of the Remote Link.
_____ All hardware and software meet approved site standards for classified processing.

ISSO Comments and Additional Assurances:

_____