5 FAH-11 H-830
ESTABLISHING NETWORK EXTENSIONS

(CT:IAH-2; 03-12-2007)
(Office of Origin: IRM/IA)

5 FAH-11 H-831 NETWORK EXTENSIONS

(CT:IAH-2; 03-12-2007)

a. Conducting Department business may require the extension of the Department's OpenNet and ClassNet networks to non-Department entities. A network extension under these circumstances is an expansion of OpenNet or ClassNet boundaries to include deployment of Department-approved hardware at a non-Department entity location. A network extension does not involve an interconnection to another system or extranet. While not requiring the formal memoranda of agreements or understandings set forth in 5 FAH-11 H-820, the establishment of these network extensions must comply with Department regulations and contract provisions, and be documented via a memorandum of agreement, contract modification, or Form DD-254, Department of Defense Contract Security Classification Specification as appropriate, between the sponsor and the non-Department entity (e.g., another U.S. Government agency or contractor housing the extension). (For agreement format examples, see 5 FAH-11 Exhibits H-831(1) - (4). The Department also uses Department of Defense Form DD-254.)

b. Department policy, 12 FAM 642.4-4, requires that both the Office of Computer Security (DS/SI/CS) and the Office of Information Assurance (IRM/IA) approve all network extensions, based on assessments of the requested extension's compliance with Department policy.

5 FAH-11 H-832 EXTENSION PLANNING

(CT:IAH-2; 03-12-2007)

a. The sponsoring bureaus planning a network extension must first develop a business case justifying the requirement. A memorandum detailing the business case should be sent to DS/SI/CS and IRM/IA stating why the extension is necessary and what Department mission the extension will support. The memorandum should also provide details on the planned extension's off-site location, point of contact at the off-site location, the extension's hardware requirements, the intended users, the estimated

support costs, and the planned site-specific security controls.

b. Requested extensions that involve contractual sites will also require contract modifications to assure protection of the Department's and other parties' interests. For classified contracts, the Contract Security Classification Specification (Form DD-254, Department of Defense Contract Security Classification Specification) must include the contractor's responsibilities for assuring the security of the extension.

5 FAH-11 H-833 REQUEST PROCESS

(CT:IAH-2; 03-12-2007)

a. DS/SI/CS coordinates the sponsoring bureau's extension request within the Bureau of Diplomatic Security (DS) (e.g., with the Office of Information Security, Industrial Division (DS/IS/IND) if the request is for an extension at a contractor site) and with the Deputy Chief Information Officer for Operations/Chief Technology Officer (IRM/OPS) and IRM/IA.

   (1) IRM/OPS, the Enterprise Network Management Office (IRM/OPS/ENM), and the Messaging Systems Office (IRM/OPS/MSO) review the extension request and make an operational assessment of the planned connection. IRM/OPS provides clearance or non-clearance on the request to DS/SI/CS.

   (2) IRM/IA reviews the request and provides co-approval or disapproval of the request to DS/SI/CS.

   (3) Upon receiving the IRM/OPS clearance and IRM/IA co-approval, DS/SI/CS provides an interim approval with security requirements to the sponsoring bureau. If IRM/OPS provides a non-clearance or IRM/IA and/or DS/SI/CS provides a disapproval, the request will be denied.

   (4) When DS/SI/CS confirms the security requirements have been met, a final approval regarding the extension is provided to the sponsoring bureau, IRM/IA, IRM/OPS, and IRM/OPS/ENM. IRM/IA must co-sign the approval.

   (5) If at any time DS/SI/CS determines that the extension is no longer in compliance with the terms of the approval, it may be revoked. The sponsoring bureau will have an opportunity to correct any deficiencies before an approved extension is revoked.

b. The interim approval memorandum should set forth terms and conditions for implementing the network extension.

c. A decision memorandum that disapproves the extension request should include the reason for the denial and the action required in order for the sponsoring bureau to obtain approval for a network extension.

d. Approvals are valid for a maximum of one year, and must be renewed in order to continue past one year. The sponsoring bureau must request a renewal at least 30 days in advance of the approval's expiration. DS/SI/CS and IRM/IA must approve and IRM/OPS must clear all renewals.

e. The sponsoring bureau must notify DS/SI/CS and IRM/IA promptly if the extension is discontinued (e.g., when the extension is no longer needed).

5 FAH-11 H-834 THROUGH H-839 UNASSIGNED

5 FAH-11 EXHIBIT H-831(1) AGREEMENT FORMAT FOR OPENNET/CLASSNET EXTENSIONS TO DEPARTMENT CONTRACTORS

(CT:IAH-2; 03-12-2007)

I. Purpose – state what the agreement authorizes and why it is necessary- include summary of business case justification

II. Contractual Authorization – cite contract provisions authorizing connection (i.e., Form DD-254, Department of Defense Contract Security Classification Specification)

III. Applicability and Definitions – characterize nature and sensitivity of data and the appropriate classification thereof

IV. Conditions and Responsibilities

- Describe method of interconnection
- Identify exact locations of connection (i.e., server connections) and purpose of user access
- Define hardware requirements and who will provide such equipment or resources
- State what organization is responsible for supporting the connection
- Estimate support costs and how they will be shared
- Define how user access is limited by router/firewall connections
- Describe incident reporting procedures
- Cite establishment of encrypted links
- Must include acceptance to comply with 12 FAM 600 security requirements

V. Security Checks

- Date of the Bureau of Diplomatic Security (DS) validation of physical security at drop location
- Date of the Information Assurance Office (IRM/IA) risk analysis
- Date of Deputy Chief Information Officer for Operations/Chief Technology Officer (IRM/OPS) approval

VI. Effective Date of Agreement – cite agreement's effective date

VII. Termination/Suspensions of Agreement

- Define procedures for terminating the agreement- who may terminate or suspend the agreement and under what conditions

VIII. Signature Blocks

For Department of State IRM	For Sponsoring Bureau
_____	_____

(Signature) (date) (Signature) (date)

5 FAH-11 EXHIBIT H-831(2)
AGREEMENT FORMAT FOR OPENNET/CLASSNET EXTENSIONS TO OTHER FEDERAL AGENCIES

(CT:IAH-2; 03-12-2007)

I. Purpose – state what the agreement authorizes and why it is necessary and include summary of business case justification

II. Authorization – cite Memorandum of Understanding provisions authorizing connection

III. Applicability and Definitions – characterize nature and sensitivity of data and the appropriate classification thereof

IV. Conditions and Responsibilities

- Describe method of interconnection
- Identify exact locations of connection (i.e., server) and purpose of user access
- Define hardware requirements and who will provide such equipment or resources
- State what organization is responsible for supporting the connection
- Estimate support costs and how they will be shared
- Define how user access is limited by router/firewall connections
- Describe incident reporting procedures
- Cite establishment of encrypted links
- Must include acceptance to comply with 12 FAM 600 security requirements

V. Security Checks

- Date of the Bureau of Diplomatic Security (DS) validation of physical security at drop location
- Date of the Information Assurance Office (IRM/IA) risk analysis
- Date of, Deputy Chief Information Officer for Operations/Chief Technology Officer (IRM/OPS) approval

VI. Effective Date of Agreement – cite agreement's effective date

VII. Termination/Suspensions of Agreement

- Define procedures for terminating the agreement- who may terminate or suspend the agreement and under what conditions

VIII. Signature Blocks

For Department of State		For Federal Agency	
(Signature)	(date)	(Signature)	(date)

5 FAH-11 EXHIBIT H-831(3) AGREEMENT FORMAT FOR OPENNET/CLASSNET EXTENSIONS TO OTHER GOVERNMENTS

(CT:IAH-2; 03-12-2007)

I. Purpose – state what the agreement authorizes and why it is necessary - include summary of business case justification

II. Authorization – cite government or International Agreement provisions authorizing connection

III. Applicability and Definitions – characterize nature and sensitivity of data and the appropriate classification thereof

IV. Conditions and Responsibilities

- Describe method of interconnection
- Identify exact locations of connection (i.e., server) and purpose of user access
- Define hardware requirements and who will provide such equipment or resources
- State what government is responsible for supporting the connection
- Estimate support costs and how they will be shared
- Describe how users are cleared for access
- Define how user access is limited by router/firewall connections
- Describe incident reporting procedures
- Cite establishment of encrypted links
- Must include acceptance to comply with 12 FAM 600 security requirements

V. Security Checks

- Date of the Bureau of Diplomatic Security (DS) validation of physical security at drop location
- Date of the Information Assurance Office (IRM/IA) risk analysis
- Date of the Deputy Chief Information Officer for Operations/Chief Technology Officer (IRM/OPS) approval
- Date of the Office of the Legal Advisor (L) approval

VI. Effective Date of Agreement – cite agreement's effective date

VII. Termination/Suspensions of Agreement

- Define procedures for terminating the agreement- who may terminate or suspend the agreement and under what conditions

VIII. Signature Blocks

For Department of State _____

For other government entity _____

(Signature) (date) (Signature) (date)

5 FAH-11 EXHIBIT H-831(4) FORMAT FOR TEMPORARY OPENNET EXTENSIONS TO OTHER NON-GOVERNMENT ENTITIES AGREEMENT

(CT:IAH-2; 03-12-2007)

I. Purpose – state what the agreement authorizes and why it is necessary
- include summary of business case justification

II. Authorization – cite legal document authorizing the connection

III. Applicability and Definitions – characterize nature and sensitivity of data and the appropriate classification thereof

IV. Conditions and Responsibilities
- Describe method of interconnection
- Identify exact locations of connection (i.e., server) and purpose of user access
- Define hardware requirements and who will provide such equipment or resources
- State what government is responsible for supporting the connection
- Estimate support costs and how they will be shared
- Describe how users are cleared for access
- Define how user access is limited by router/firewall connections
- Describe incident reporting procedures
- Cite establishment of encrypted links
- Must include acceptance to comply with 12 FAM 600 security requirements

V. Security Checks
- Date of the Bureau of Diplomatic Security (DS) validation of physical security at drop location
- Date of the Information Assurance (IRM/IA) risk analysis
- Date of the Chief Technology Officer, Deputy Chief Information Officer, Operations (IRM/OPS) approval
- Date of the Office of the Legal Advisor's (L's) approval [required if agreement is with a foreign non-government entity]

VI. Effective Date of Agreement – cite agreement's effective date

VII. Termination/Suspensions of Agreement
- Define procedures for terminating the agreement- who may terminate or suspend the agreement and under what conditions

VIII. Signature Blocks

For Department of State _____

For non-government entity _____

(Signature) (date) (Signature) (date)